# EXCHANGE 2000 CONFERENCING SERVER


**EXCHANGE 2000 CONFERENCING SERVER....1**

**EXCHANGE 2000 CONFERENCING SERVER....4**

**KEY TERMINOLOGY....6**

**INTRODUCTION....7**

WHAT BUSINESS PROBLEMS DOES CONFERENCING SOLVE....7

*Co-ordination of conference invitations:....8*

*Finding a conference host:....8*

*Creating the conference topology:....8*

*Security and encryption:....9*

*Conferencing across a firewall:....9*

*Working within limited resources:....10*

TARGET SCENARIO....10

**EXCHANGE 2000 CONFERENCING SERVER OVERVIEW....12**

FEATURE OVERVIEW....12

*Outlook Calendar:....12*

*Conference Window:....13*

*Conference Management Service:....13*

*Data Conferencing Service:....14*

*Video Conferencing Service:....15*

*Server Management Console:....16*

*Exchange 2000 Server Integration....16*

EXCHANGE 2000 CONFERENCING SERVER ARCHITECTURAL OVERVIEW....17

*Conference Management Service....19*

*Conference Technology Providers....19*

*Support for 3rd party providers....19*

*Conference Access Pages....19*

*Exchange T.120 Multi-point Control Unit....19*

*Exchange H.323 Videoconference Bridge....20*

*Exchange 2000 Server....20*

*Windows 2000 MADCAP Service....20*

*Windows 2000 Certificate Server....20*

*Windows 2000 Active Directory....20*

*Microsoft Management Console....21*

*Windows Client....21*

SECURITY OVERVIEW....21

*Reservation and scheduling....21*

Permission to directly book a resource....22

Permission to invite a resource....22

Accessing the conference location (URL) 22
Participation in a conference 23
*Administration* 24
Windows site-based service 24
Administration Groups 25
Service Management 25
Logging reports 25
*Client Overview* 26
Requirements to participate in a conference 26
*Outlook 2000 integration and configuration* 27
Deployment Overview 28
Installation Overview 29
Best Practices 31

**CONFERENCE MANAGEMENT SERVICE 32**

What is the Conference Management Service? 32
*Scheduling a conference:* 32
*Joining a conference:* 32
Deployment strategies 33
*Placement of Conference Technology Providers* 34
*Conference Access via IIS* 34
*Defining the default conference access location* 35
*Scalability* 35
*Reliability Planning* 35
*Backup/Restore strategy* 36
Conference Management Security Model 37
*Public and Private Conferences* 37
Conference Access Control 37
Security Supplied by CTP 38
*Resource Management* 38
Defining the conferencing experience 38
*Naming Conventions* 39
*Configuring Resources* 40
*When is a resource busy* 40
Conference Calendar Mailbox 40
Conference Access Pages 41

**DEPLOYING THE CONFERENCE MANAGEMENT SERVICE 43**

Server Requirements 44
Administration 45
*Permissions* 45
Exchange Conferencing Management and Providers 45
Conferencing Server Services 45
Resource Management 45

**EXCHANGE DATA CONFERENCING SERVICE 46**

What is Data Conferencing? 46
*Joining a data conference* 47
*What is an MCU?* 48
Resource Properties Settings 48
Data Server Deployment Topology 49
*Windows Site Architecture* 49
*Placement of Conference Management Services* 50
*Corporate network topology and bandwidth characteristics* 50

*Network location of conferencing users* ..... *50*
*Requirement to conference with users across a firewall* ..... *51*
*Bridging of Videoconferences* ..... *51*
SITE ARCHITECTURE ..... 52
BACKBONED NETWORK ..... 53
HUB AND SPOKE ..... 53
DEPLOYMENT IN MULTIPLE SITES ..... 54
MCU Connections and Types ..... 56
Security Model ..... 57
Reliability Planning ..... 58
Scalability and Performance ..... 58
Deploying Data Conferencing ..... 58
**EXCHANGE VIDEO CONFERENCING SERVICE ..... 60**
What is Video Conferencing? ..... 60
What is MADCAP? ..... 61
What is IP multicast? ..... 62
What is a multicast address? ..... 62
What is TTL? ..... 62
What is a multicast group? ..... 62
What is a multicast scope ..... 63
Reserved addresses: ..... 63
How to use Scope/TTL to limit video on your network ..... 64
Reliability Planning ..... 64
Configuring routers on your network ..... 65
Resource Properties Settings ..... 65
Network considerations ..... 67
Deploying Video Conferencing ..... 67
Clients ..... 68

# Exchange 2000 Conferencing Server

The Exchange Conferencing Server is an exciting new companion product for Exchange 2000 Server.

The Conferencing Server provides the functionality to extend Exchange 2000 Server into the area of real-time collaboration. The Conferencing Server highlights three specific area of real-time collaboration that together offer businesses, both large and small alike, key benefits in the empowerment of their knowledge workers.

### Conference Management

At the center of the Conferencing Server is the Conference Management Service (CMS). This component is responsible for the overall coordination and management of different conferencing technologies and administration of conferencing resources. CMS keeps track of scheduled conferences and provides means to control attendee's access to conferences. CMS is an extendible platform for variety of conferencing technologies that can be developed by independent software vendors and installed along with the Exchange 2000 Conferencing Server (ECS).

### Data Conferencing

Data Conferencing Service (DCS) is a conference technology that provides for multiparty application sharing, chat, whiteboarding and file transfer capabilities based on T.120 ITU-T Recommendation for Multimedia Conferencing.

DCS creates, transparently for the end users, a data conference environment optimizing conference performance and network resources' utilization, bridging participants from remote sites and across firewalls.

### Video and Audio Conferencing

Video and Audio Conferencing Service (VCS) is a conference technology that provides multiparty video/audio conferences over multicast enabled IP networks. VCS provides network bandwidth efficient way of distributing audio/video traffic among conference participants.

When used in combination with the DCS it is possible to bridge NetMeeting clients using H.323 unicast audio/video standard into the VCS multicast conference.

ECS is a platform for additional conferencing types that, when installed; seamlessly integrate into a unified user experience adding new functionality and capabilities to the existing service. With ECS, you can combine any number and combination of conferencing types that will instantly become available to the conference participants when they join the conference. As an example: a telephone conferencing provider can be installed and a conference scheduled against a resource with data and telephony capabilities. Participants will join the conference with one click of the mouse and be able to share a desktop application and communicate via telephones.

The remainder of this document will describe the components of the ECS, their functionality, architecture, deployment strategies and requirements, reliability and security issues and more.

# Key Terminology

- **Exchange 2000 Conferencing Server (ECS or Conferencing Server)** is a companion product to Exchange 2000 Server enabling real-time multiparty online conferences.
- **Conference Management Service (CMS or conference manager)** is a central component of the Conferencing Server and serves as a platform for different conferencing technologies. It is also responsible for the reservation and scheduling of online conferences.
- **Conference Technology Providers (CTP or technology providers)** are modules that extend the CMS to provide the technologies required to host online conferences. Typically, a provider specializes in a specific aspect of collaboration such as telephone or videoconferencing. CTPs can be developed by third parties and installed over ECS.
- **Data Conferencing Service (DCS)** is a CTP that provides multiparty data conferencing services, such as: application sharing or whiteboarding. DCS is a component of ECS.
- **Video Conferencing Service (VCS)** is a CTP that provides multiparty video and audio conferencing services. VCS is a component of ECS.
- **T.120 Multi-point Control Unit (MCU)** is a service used by the DCS to host client connections to its data conferences. This ECS component can be installed on one or more servers in a conferencing site on the same server as, or separate from any Conferencing Server.
- **Conferencing Site** is the administrational unit for the Conferencing Server. A Conferencing Site is defined as a Windows 2000 Site that contains a Conferencing Server running the Conference Management Service. A conferencing site may extend beyond the Windows 2000 site when a technology provider, for example the DCS, places its servers in additional Windows 2000 sites and associate them with the CMS in the root site.
- **Conference Resources** are mailbox-enabled accounts created within a Conferencing Site that are used by the Conference Management Service to facilitate reservation and scheduling of the services of Conference Technology Providers.
- **Host Server** is the Conferencing Server running the active instance of a Conference Management Service.
- **Conference Calendar Mailbox** is a dedicated Exchange 2000 mailbox used by the Conference Management Service to persist the reservation and definition of all scheduled conferences.
- **Conference Access Pages** are a set of web application pages hosted by Microsoft Internet Information Server to facilitate client access to ECS conferences.

# Introduction

Microsoft Exchange 2000 Conferencing Server provides an extendable platform for real-time online conferencing services. It allows users to structure online conferences by reserving Conference Resources, listing and inviting attendees, and setting persistent properties for each conference. Exchange Conferencing Server is shipped with two technologies in support of conferencing: Data Conferencing Service (DCS) based on T.120 protocols, and Video/Audio Conferencing Service (VCS) based on IP multicast protocols as implemented in TAPI 3.0. Technologies that integrate into the Conferencing Server are known as Conference Technology Providers (CTP).

Users can schedule and hold regular online conferences that provide live audio and video and offer features such as white boarding, chat, application sharing and file transfer. Conferences can be public or private, and can host two or more people.

The Conferencing Server centralized reservation system allows users to schedule and join conferences from the Outlook calendar. Alternatively, non-Outlook users can join conferences from a web browser, following the conference location URL included in the conference request message. A web-based conference scheduler is also available as a convenience user interface for non-Outlook users. Conferences are hosted and managed by an Exchange server, not by a client computer. Finally, its videoconferencing technology allows all conference participants to see and hear each another simultaneously, eliminating the need for a parallel teleconference.

The Conferencing Server provides the means for third-party developers to develop and add their own conferencing technologies by implementing a CTP. For example, a telephony component or a conference recorder can be developed to enhance or complement the service’s built-in technologies.

# What business problems does Conferencing solve

Exchange 2000 Conferencing Server is designed to extend the messaging and collaboration services of Exchange 2000 Server into the realms of real-time collaboration.

The Conferencing Server integration with Outlook and Exchange Server calendar features has provided the knowledge worker a seamless shift from scheduling and participation of the typical meeting held in a meeting room, into a structured online conference held in virtual meeting room hosted by the Conferencing Server.

Today, meeting online solely using applications such as NetMeeting can be a complex and troublesome experience.

# Co-ordination of conference invitations:

With today's technologies, when scheduling a time for the conference, both: conference organizer and attendees need to enter specific information about the conference. For example they need to indicate which ILS server to use, the name of the attendee server to call, will someone be using NetMeeting to invite them, or will they need to call someone to get into the conference. Typically, this information is different for each invitee.

The Conferencing Server is integrated into Outlook calendaring and encapsulates all the information required to connect each participant with the conference using Single-Click Join. Neither conference organizers nor attendees need to know anything about the servers and underlying technologies.

# Finding a conference host:

There are two models for conferencing, peer-to-peer, where participants of the conference interconnect establishing direct links between their desktops, and client-server, where participants interconnect via a central server. Today, both models require the organizer and all participants to know and work with the selected connection type. The host of the conference needs to be available for the entire duration of the conference. This may not be a problem for the server portion of the conference, but, when in peer-to-peer mode, this can be difficult for specific users that may need to leave early. However, even with the server-hosted conferences, there are problems: if the server for some reason is unavailable at the scheduled time of your conference, your online conference won't happen unless a new conference is scheduled on another server.

The Conferencing Server abstracts the hosting of a conference until the scheduled conference time, and will automatically select a load-balanced, 'best' available server for the job.

# Creating the conference topology:

Any current conferencing user is aware of the impact their online conference has on their network. Either through a technical understanding of the data passing through routers and on the wire between locations, or simply by the unacceptably slow performance they observe when too many users connect to the wrong conference host; they have to learn about conference topologies to have successful conferences.

Take a moment to look at an example. A conference organizer, on a modem in a hotel in New York, needs to invite five people from the company offices in Atlanta and five people from the offices in London. If the simplest, peer-to-peer hosted conference is created, the organizer on the modem will be continually sending ten copies of the conference information down the modem link. The 28.8 modem will now look like a 2400-baud modem. Since this organizer is using RAS into the company offices in New York, this same ten copies of data are coming into New York across the company WAN links, with the five copies of the data from London also been sent over the slow transatlantic WAN connection.

For the conference to be successful, someone in both Atlanta and London needed to host the conference participants from those locations and then interconnect the two groups so only a single copy of the data traveled across the WAN links. The organizer in the hotel in New York could then connect into one of these hosts to complete their conference topology. Great, but due to technical issues in the protocol used for in their conference, users need to interconnect in a specific order to ensure persistence of the conference.

With Exchange 2000 Conferencing Server (ECS), the optimal data conference topology is created automatically and completely transparently for the users. ECS includes a service that builds the topology dependent on the clients network locations when they join the conference - all part of the client's One-Click Join conferencing experience.

# Security and encryption:

Even if the Conferencing Server is used solely between participants within a secured intranet, it is often required to ensure only the invited people will participate and that only those participants be able to see the information discussed in an online conference. When scheduling the online conference from Outlook 2000, the organizer is offered three levels of security for their conference. These three levels, in increasing level of security, are:

Public: Allow attendees that are external to the conference invitation to attend the conference. In effect, any user that knows the address of the conference is granted access to the conference.

Public with Password: Allow the organizer to place a simple text password on this 'public' conference. Again, anyone that finds the conference location is granted access if the password is entered correctly. Typically, although in reality dependent of the technology providers hosting the conference, these two formats of conferences do not dictate that the conference contents are encrypted.

Private: The organizer indicates, on the conference schedule, that solely attendees included in the conference invitation are allowed access to the conference. Again, the level to which the conference content is encrypted is defined by the technologies that are hosting the conference. The Exchange Data Conferencing provider for example will use an SSL public certificate to authenticate users into the conference and subsequently encrypt all transmitted conference content.

The Conference Manager can be configured for private conferences to challenge for authentication any user that accesses the conference link to ensure they have access to the conference. This feature can be enabled from the VCS or DCS property settings.

# Conferencing across a firewall:

To meet with people online it is necessary to share a common network. The Internet has become the network on which this connectivity has been achieved. Along with the people on the network you do want to share information with, however, there are a large number of people with which you don't. The company firewall is the barrier that is installed to block the free flow of information in and out of the company. This information-flow barrier however is also a barrier to the information flow within an online conference.

Through a correct deployment of Conferencing Servers, this barrier to communications can be bridged in a controlled and secure manner to enable online conferences with attendees outside the company firewall.  In addition, the intent of the Conferencing Server is to make each conference attendee's participation in an online conference seamless, regardless of their location on the broader Internet.

## Working within limited resources:

A building within a company has only a limited and defined number of meeting rooms in which meetings can be held.  Put meetings in every room and the ability of the building to host another meeting is exhausted.  To avoid chaos and confusion, the usage of these meeting rooms would typically be scheduled so that the meeting organizer can be happy that the room is reserved for their meeting.

Even though the online conference does not have a physical location in which people meet, these virtual conferences do still place demands on the company infrastructure in terms of network and server load.  The cost on the infrastructure of a virtual meeting is dependent on the type of online conference.  An online conference that is solely accomplished using the telephone, places a demand on the company resources differently than an online videoconference would place on the company network.

The Conferencing Server achieves an abstract resource model by administration of conferencing technology providers and through the scheduling and reservations of their associated resources.  The organizer of an online conference can therefore have the same comfort level as he has when scheduling against a physical meeting room.

The company IT group typically provides the resource required to host an online conference. Through the Conferencing Server resource model, they can also define and manage their conferencing infrastructure to support the demands of the online conferences within the company.

# Target Scenario

The scope of what can be accomplish by groups of knowledge workers when enabled to move their meeting online can be significant to both the user and the company in which they work.

The ability to meet online builds team interaction that otherwise would be impossible or difficult when separated by geographical distance. With the workers of an enterprise typically spread across the nation, or even the globe, the Conferencing Server becomes their bridge, pooling the knowledge of everyone in the company.  Workers with specialized knowledge can participate in conferences at the other side of the world without the need to take, possibly, days to travel to the conference.  The barriers of distance are removed.

Meetings that bring such workers together typically are very structured; they have a documented agenda, the goals of which are to be accomplished on a specific day, at a pre-specified time. This type of meeting often has a limited or restricted list of named participants. The meeting organizer needs to ensure that

everything is in order prior to event.  Finding another meeting already going on in the room, or the room having been taken out of service for an upgrade of the decor is not acceptable, especially when many people may have traveled many miles.  Needing to find an alternative venue at the start of your meeting is a waste of everyone's time.  The meeting location needs to be found easily.  Having to telephone for directions is disruptive, if possible at all.  Participants need clear instructions of when, where and what the meeting is all about and must be given the ability to attend with minimal overhead or disruption to the rest of their day.

The Conferencing Server strives to ensure its virtual, online conferences meet and often exceed this existing structured meeting metaphor. From within the organizer calendar, the user can schedule the date and time of the conference and specify the conference agenda.  Instead of reserving and finding an available physical meeting room, the organizer, while still within the Outlook address book, can invite a Conference Resource, the virtual meeting room.  The server ensures that the conference invitations are not sent if the technology to host the conference is not available at the specified time – if it is available, the server ensures that it will be still available when the conference starts. For a closed, or private, conference, the organizer can identify the conference as such by limiting it from attendees that are external, that is, are not on the conference's attendee list.

When the conference is due to start, a conference reminder allows each participant to join the online conference with a single click of a mouse, regardless of where the conference was scheduled or the technologies used.  The Conferencing Server looks at each user when they attempt to join a conference and confirms they have permission to join before offering details of the conference.  The server, in addition, inspects the user's physical network location and which applications they have available on their computer and offers the best experience available by connecting them to local servers automatically.

# Exchange 2000 Conferencing Server Overview

## Feature overview

As a companion product to Exchange 2000 Server, the Conferencing Server enables collaboration between corporate knowledge workers in real-time. Constructed from a number of inter-related services, the Conferencing Server creates a complete and extensible environment in which to conduct collaboration, online, in real-time.

By means of integration into Outlook, the server enables the user to schedule and reserve online-conferences. This action automatically reserves the resources required to support the conference.

The following section offers an overview of the features delivered by each of the components of the Conferencing Server.

## Outlook Calendar:

Outlook 2000 includes as an integral part of calendaring, the ability to schedule an online conference against the Exchange Conferencing Server. On the Outlook conference form, an option allows the conference organizer to mark the meeting as online using Exchange conferencing.

From within the company address book, the organizer can invite a Conference Resource as the resource of the meeting. This, in effect, is the virtual meeting room in which the conference will be held.

Outlook 2000's ability to directly book resources is used to confirm the reservation of conference resources prior to sending the attendees the conference invitation.

A link (URL) to the online conference is included in each invitation that's sent to the conference participants. Attendees can access this link with a browser to join the conference. Outlook 2000 users will receive as normal, a conference reminder for the online conference that includes an additional button titled, *join conference*. Selecting *join conference* will automatically initiate the attendee's participation in the conference. In addition, the join conference action is also available before and after the conference scheduled start time from within Outlook's context menu and toolbar selections. Joining a conference early may provide information about the conference, joining late may provide, for example, a recording of the conference. Such functionality is dependent on the technology provider that hosted the conference.

Online conference organizers without the ability to directly book online conferences using Outlook 2000 have two alternatives to schedule online conferences. Using a previous version of Outlook the conference resource can be invited as a normal attendee of the conference from the Outlook conference request form. Likewise, using Exchange Outlook Web Access (OWA) or the new Exchange 2000 web client, a conference organizer can invite the resource as a conference attendee. However, unlike the Outlook 2000 organizer, when using these methods it is impossible to identify the conference as private and as such all conferences will allow non-invited attendees. In addition, the conference location, or URL link, is not automatically included in the initial conference invitation. It is the organizer's responsibility to

forward the URL to all conference attendees. This URL is included in the conference accept message from the Conference Manager.

# Conference Window:

The conference window is presented to conference participants when they access the conference link, (URL). This conference window, hosted in an Internet browser, will display a framed page that will look different dependent on used conferencing technologies and whether user accesses the conference before, after or during the conference scheduled time. The leftmost frame of the conference window, called *conference panel,* displays general information about the conference. There are one or more additional frames, each associated with a specific conference technology provider. The set of conference technologies available in a conference is defined by a conferencing resource selected at the scheduling time.

The Conference Panel provides to each participant, information including:

- The conference schedule and time remaining;
- A mail-enabled link to the conference organizer;
- The conference subject;
- Indication on whether the conference is private (attendance is restricted to only the invitees);

For the conference organizer, the following links, dependent on configuration, are available:

- Request to extend the length of the conference in session;
- Request to change the resource, or virtual room, in which the conference is hosted. This is typically required to increase the size of the room to allow additional participants.

The Conference Window will warn the participants 5 minutes prior to the automatic termination of the conference. At the end of the 5-minute period, participants are forcibly disconnected from the conference resources, unless a grace period is set and is honored by the providers. Grace periods can be set for before and for after the scheduled conference time, and are convenience tools to allow attendees to arrive early or leave conferences late. Grace periods are set by administrators and apply to all scheduled conferences.

# Conference Management Service:

The Conference Management Service (CMS) is the component of the Conferencing Server that is responsible for the management of Conference Resources and the facilitation of Conference Technology Providers.

Together with a web site hosted on Microsoft Internet Information Server (IIS), the Conference Management Service provides the client access to online conferences. These web pages can be configured to require user authentication and subsequently limit access to a privately scheduled conference to only invited attendees.

Conference Resources are mailbox-enabled objects published in the Active Directory, the Conference Management Service publishes their availability via the

Exchange Server free/busy mechanism. Outlook uses this information to indicate to users the ability to schedule a conference at a specific time.

When a conference is schedule, the management service provides the URL that is to be used to access the conference by inserting it into the Outlook invitation. A complete store of all scheduled conferences are held by the management service in the Conference Calendar Mailbox. This store is used to create a persistent representation of the conference format and structure and any additional information associated with the conference.

The CMS also provides the interfaces to allow the scheduling of reservations from email clients that do not support direct booking.

The lifetime of an online conference is controlled by the CMS. This service works in co-operation with each technology provider to ensure that the conference starts and ends in accordance with the conference organizer's wishes.

The CMS keeps a list of all conferences scheduled using the conference resources it defines. Any publicly scheduled conferences also appear on the conference event calendar allowing any web client the ability to browse into the conference (assuming they know any defined password). Private conferences are not listed. In order to join a private conference participants are required to explicitly know the URL of the conference.

The CMS allows the server administrator to historically analyze the schedule and conference activities from an audit log file. This formatted, comma-delimited file is created for each day and is available on the Conferencing Server hosting the active Conference Management Service. For the description of the format of these files, see the ECS online documentation.

# Data Conferencing Service:

DCS is a technology provider that delivers, within an online conference, the facilities to share applications, conduct whiteboard sessions, chat and transfer documents. This data collaboration is accomplished using tools such as Microsoft NetMeeting or any other applications that support the T.120 network communications standard. The precise client experience for the version and vendor of the application define data conferencing used within the online conference.

The DCS creates a resource scheme based on a count of how many simultaneous conference participation connections it will permit in any online conference at the same point in time. This maximum participation count is the physical resource against which the conferencing resource requests reservations when it is invited to an online conference. Each DCS conferencing resource has a size associated with it. The Conferencing resource considers this 'size' as the cost of hosting the conference. The DCS will place this cost against the maximum participation count. If the available count reaches zero for any specific time, then the DCS will cause the Conference Manager to publish a busy indication to the users and no additional reservations will be accepted.

Each data conference participant's computers is connected to a T.120 multi-point control unit, or as more commonly referred to, an MCU, when attending a data online conference. Within the Conferencing Site, the T.120 MCU can be installed on multiple Windows 2000 servers and may be grouped into clustered farms of servers at a specific conferencing site. This farm of MCUs provides the platform on which each scheduled data conference will be hosted. When a data

conference participant joins a conference, the DCS tries to select the ‘best’ MCU taking into account the following set of criteria:

- Which MCUs are available and in service?
- Is the conference already running on a MCU?
- What’s the load that existing conferences are placing on the MCU?
- Are there any administratively defined restrictions on which MCU can be used?
- The network location of the user within the Conferencing Site,
- Whether the user is inside the local Conferencing Site,
- Is the user closer to another Conferencing Site,
- Whether the user is outside the organizations network

Using these criteria, the DCS attempts to refer a user connecting to a conference to an MCU that is closest to their network location and that will limit the number of copies of the conferencing data sent between these locations. Since the MCU selection is made at participant join time, the subsequent interconnection of MCUs, the conference topology, is dynamic and can optimize the ambiguity of server availability and user network location.

When the client has NetMeeting 3.01 or above installed, the DCS will place the controls for NetMeeting within the conference window’s browser frame (given the browser is capable to host ActiveX controls). Both Internet Explorer 4.01 and NetMeeting 3.01 or above are required to join a private conference using a public key certificate for authentication and encryption of the data transmitted.

The T.120 multi-point control unit can be installed independently of other services. Each MCU automatically attempts to retrieve a machine certificate from a Windows 2000 certificate server so that it can host private conferences by authenticating the connection between both MCU and clients when building the conference topology. Without a valid certificate, the DCS cannot host a conference that is restricted to conference attendees only, the private conference.

# Video Conferencing Service:

VCS is a technology provider that delivers the facilities to both hear and see each conference participant within an online conference. This collaboration is accomplished using either the Exchange videoconferencing client or Microsoft NetMeeting. These clients either join the multicast backbone of the conference directly, or are bridged using a H.323 call, respectively.

The VCS creates a resource scheme based on a count of how many simultaneous conference participants are invited to online conferences at the same point in time. This maximum participant count therefore defines the maximum number of audio/video data streams that can be sent across the network at any point in time.

Each VCS Conferencing Resource has a size associated with it. The resource considers this ‘size’ as the cost of hosting the video portion of the conference. The VCS will place this cost against the maximum participation count. If the available count reaches zero for any specific time, then the VCS will cause the

Conference Manager to publish a busy indication to the users and no additional reservations will be accepted.

Each resource can also define actual format the videoconference will take. The following properties can be set on a per videoconferencing resource basis:

- Whether the G.711 or GSM6.10 CODEC is used for transmitting audio,
- Whether video is enabled within the conference (audio-only conference),
- Whether the H.261 or H.263 CODEC is used for transmitting video,
- The size of the video image, QCIF or CIF,
- Is audio and/or video automatically sent for a participant when they first join a conference
- What is the advertising scope (which of the Multicast scopes could be used) for the videoconference
- Whether H.323 bridging is permitted

For a conference in which all participants are directly connected to the multicast videoconference, no server or MCU is involved in delivery of the conference information to the participants. The video conferencing provider logic does however still monitor the conference and will ensure no more participants than the number defined by the reservation count may join the conference.

If a participant can not connect directly to the multicast streams and the DCS is also involved in the online conference, then the VCS asks the DCS to supply a bridge between the multicast streams and a H.323 call from the participant.

# Server Management Console:

Configuration of the Conference Management Service, providers is achieved through a Microsoft Management Console (MMC) snap-in. This Conferencing Server snap-in can be installed and run remotely to the Conference Server. Administration activities can also be accomplished when the server or services are offline.

All administration and configuration data are stored in the Windows 2000 Active Directory enabling multi-master administration of the service.

# Exchange 2000 Server Integration

The Exchange Conferencing Server can be natively installed directly into an Exchange 2000 organization. To enable the conferencing services for users within an Exchange 5.5 organization, it is necessary to first install and deploy at least one Exchange 2000 Server within the existing Exchange 5.5 organization.

An Exchange 2000 Server can be installed in either an existing 5.5 organization or a new Exchange 2000 organization. The Conferencing Server is therefore always installed into the organization containing an Exchange 2000 Server.

Refer to the Exchange 2000 Server documentation for information in installing Exchange 2000 Server.

Since the CMS publishes free/busy information for each Conferencing Resource, the CMS must have access to the Exchange free/busy public folder. Typically, this is

achieved by ensuring the domain in which the CMS exists includes an Exchange replica of the free/busy public folder for the organization.

# Exchange 2000 Conferencing Server Architectural Overview

Exchange Conferencing Server consists of the following components and services:

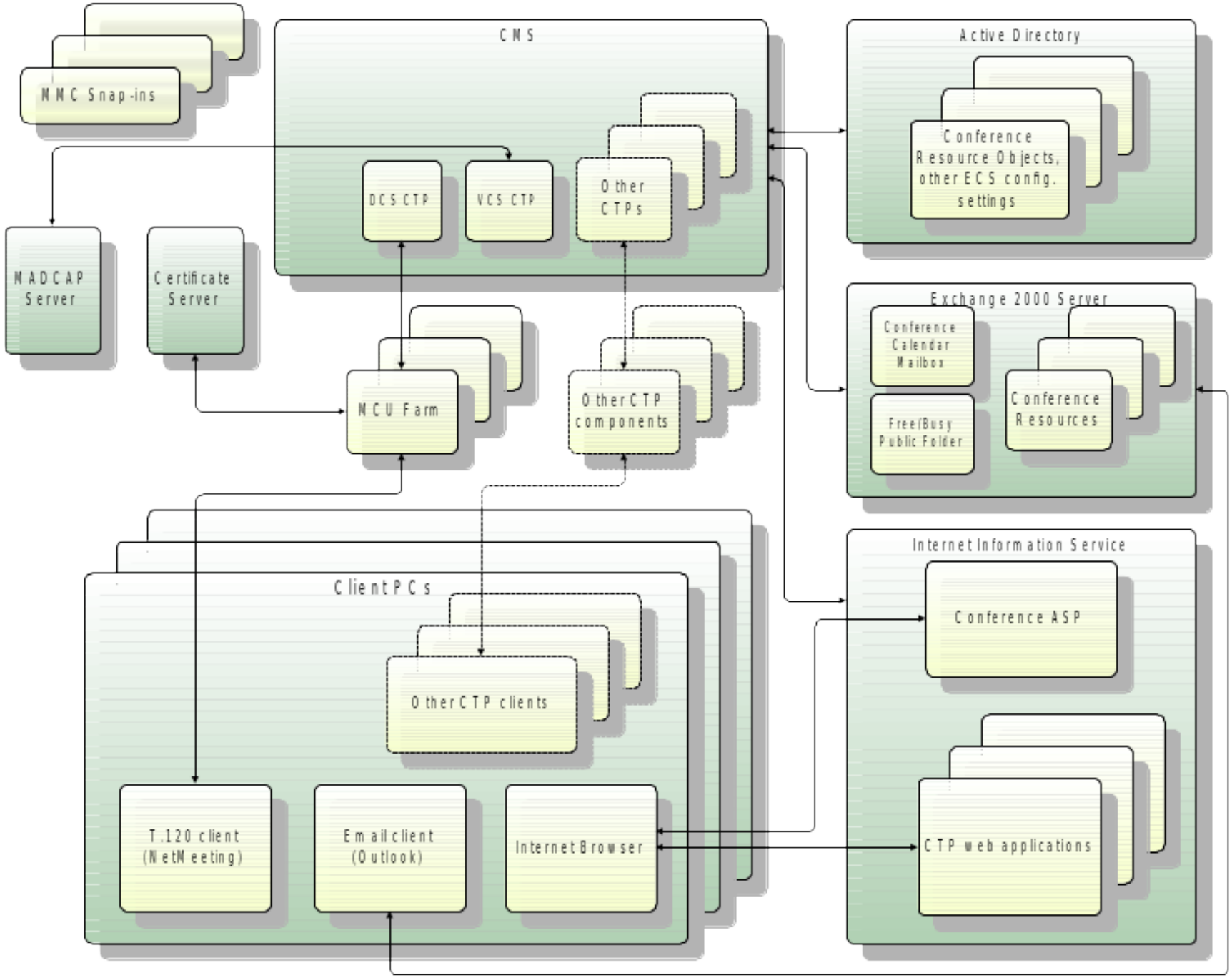
- Exchange Conference Management Service
- Conference Technology Providers, that include
- Exchange Data Conferencing Service
- Exchange Video Conferencing Service
- Support for 3rd Party Providers
- Conference Access Pages hosted on Microsoft Internet Information Server (IIS)
- Exchange T.120 Multi-point Control Unit
- Exchange H.323 Videoconferencing Bridge
- In addition, the Conferencing Server requires the following components and services:
- Exchange 2000 Server
- Windows 2000 MADCAP Service (required for VCS only)
- Windows 2000 Certificate Server (required for private conferences only)
- Windows 2000 Active Directory
- Microsoft Management Console

Recommended client configuration:

- Windows client (Windows 2000 or higher recommended)
- Internet browser (Internet Explorer 4.01 or higher recommended)
- Email client (Outlook 2000 or higher recommended)
- T.120 client (NetMeeting 3.01or higher recommended)

A functional diagram representing the listed services and their interrelationship in a Conferencing Site is depicted below.

# Conferencing Site Functional Diagram



# Conference Management Service

**Conference Management Service** enables the conference technology providers and allows for the management of conference resources, scheduled conference profiles and duration, and attendee access rights verification.

The CMS controls the client's access to all online conferences scheduled with the service. This client access is achieved via Microsoft Internet Information Server through a web site installed as part of the CMS installation.

# Conference Technology Providers

Exchange 2000 Conferencing Server includes two Conference Technology Providers:

- **Data conferencing service (DCS)** is a conference technology provider consisting of a controller, which must be installed on a server where the CMS is installed, and one or more T.120 Multi-point Control Units. MCUs can be installed on a separate server with no other Exchange components installed. T.120 MCUs serve as nodes for T.120 data conferences. Increasing the number of MCUs on a site increases the data conferencing capacity of that site and allows the "Maximum Number of Scheduled Connections" setting of a Data conferencing provider to be increased. For more information, refer to the Exchange 2000 Conferencing Server online documentation.
- **Video conferencing service (VCS)** is always installed with the CMS; however, Windows 2000 MADCAP services must be present in the network in order for video conferencing to function. For more information, see "Video Conference Planning and Configuration" later in this chapter.

# Support for 3rd party providers

In addition to the two CTPs available with the Conferencing Server, providers are available from other companies that allow the integration of their conferencing products within the Exchange Conference Management Services.

Such conferencing technologies may include telephone conferencing, H320 ISDN video bridging, presentational events and more.

# Conference Access Pages

The Conferencing Server utilizes IIS to host the HTML pages used by conference participants to join and interact within an online conference. Access control, the restriction of only invited participants to online conference is also implemented on the IIS conference access pages.

# Exchange T.120 Multi-point Control Unit

This service runs as a component of the Data conferencing provider and is used to interconnect network connections between participants in a data conference.

It communicates with the DCS controller through a DCOM session and with conference participants through the T.120 protocol.

# Exchange H.323 Videoconference Bridge

This service runs as a component of the T.120 Multi-point Control Unit and permits clients with NetMeeting unable to directly connect to the multicast conferences hosted by VCS to connect through a H.323 unicast session.

# Exchange 2000 Server

- The Conferencing Server utilizes the storage capability of Exchange Server to hold the definition and reservation of online conferences. This integration allows administration of Exchange Server, such as backup policies, to unify such requirements of the Conferencing Server.
- The Conferencing Server has two types of mailboxes hosted by Exchange Server, the Conference Calendar Mailbox and the Conference Resources. The calendar mailbox is a storage location used to persist the definitions and structure of all conferences. The Conference Resources are the mailboxes users invite to a conference to reserve the facilities of the CTPs hosting the conference.

# Windows 2000 MADCAP Service

- The Exchange Video Provider requires the services of MADCAP integrated into the Windows 2000 DHCP allocation of network addresses within the corporation's network. The multi-cast addresses retrieved from MADCAP are used by the videoconference to define the scope, that is to say, the network region in which a videoconference exists.

# Windows 2000 Certificate Server

The T.120 Multi-point control unit utilizes the Windows certificate server to enroll into the X509v3 public certificate mechanism. The MCU uses these certificates to support the access controlled online conferences to allow authentication on connections with other MCUs and client participants.

Conference invitees may use the Windows 2000 Certificate Server to obtain their own client certificates for use by NetMeeting 3.01 in order to join private conferences.

# Windows 2000 Active Directory

In common with Exchange Server, the Conferencing Server places all configuration information within the Active Directory. This facilitates multi-master, remote and offline administration. The Conferencing Server also uses information in the active directory to understand the network topology.

# Microsoft Management Console

The Conferencing Server and associated providers use the Microsoft Management Console to facilitate system administration.

# Windows Client

In addition to the Conferencing Server's use of many Windows 2000 Server services, the best client experience for conferencing comes from the integration of Outlook 2000, Internet Explorer, NetMeeting and the TAPI telephony libraries for multicast videoconferencing.

# Security Overview

The Exchange 2000 Conferencing Server provides various aspects of security to limit user access to the Conference Resources and participation in online conferences.

- This security can be split into three separate areas:
- Ability to reserve resources for an online conference
- Ability to access an online conference
- Ability to participate in an online conference
    - Since the hosting CTP defines the act of participation in an online conference, the provider defines the specific format of any conference security. The creation and access to conferences is controlled by the Conference Manager and is therefore consistent across all providers.

# Reservation and scheduling

To create an online conference on the Exchange 2000 Conferencing Server it is necessary to reserve the resources required to host the conference.

The CTPs work together with the Conference Manager to publish the availability of their resources. This availability is made visible to the conference organizers through the standard Outlook/Exchange free/busy publishing mechanism. If a provider has indicated that a resource is busy, then no conferences can be scheduled against that resource for that time.

The scheduling of Conference Resources is accomplished via one of two basic mechanisms:

***Confirmed reservation*** is achieved from a Client such as Outlook 2000 whereby the resources are directly-booked into the conference prior to the invitations been sent. If the resource is not available then the invitations are not sent.

***Asynchronous reservation*** is achieved by sending an invite to the conference via email to the resource. If the resource is available, the organizer receives from the resource an acknowledgement email that accepts the reservation and provides the conference URL.

# Permission to directly book a resource

The scheduling agent, such as Outlook 2000, atomically opening and writing into the resource's calendar achieves the act of "Confirmed Reservation". Outlook 2000 also can be configured for this action on typical meeting rooms.

To restrict who can directly book a resource is achieved by applying permissions for named users or security groups to the resource calendar folder. To deny access, a user or group should be given *access=none*, to allow access they should be given *access=author.* The CMS defaults a resource to *Default=Author* to enable access for all users.

These permissions are applied directly from an Outlook client logged into the resource mailbox by selecting the properties of the calendar folder.

# Permission to invite a resource

Any application capable of sending an appointment invitation to a mailbox can asynchronously schedule the reservation of resources.

Applications capable of sending appointment invitations include:

- Outlook 95, Outlook 97, Outlook 98 and Outlook 2000 if in offline mode
- Exchange 5.5, Outlook Web Access
- Exchange 2000 Web Client
    - In all cases, to restrict who can book a resource in this manner, apply Exchange delivery restrictions to the mailbox associated with the resource.
    - These permissions are applied from the Windows 2000, User and Computer management console from the Exchange General tab on the resource property page.
    - The mailbox objects associated with the Conference Resources are created in the **Exchange Resources** folder found under the **System** organizational unit. To view this node, the management console must be placed in 'advanced features' view mode.

# Accessing the conference location (URL)

The location of each online conference is defined by a unique URL of the form of:

http://<server>/<root>/<conference id>

The CMS along with its associated IIS is responsible for rendering the conference location into a set of html pages capable of offering participation in an online conference.

When the organizer schedules the online conference, they also define the level of access for the conference via two basic constructs, those of a public or private conference. A public conference is published on the Conference Manager's web site and is visible to any user. This allows, therefore, participation from users that are external to the conference attendee list. External attendees are not permitted in a private conference and the conference is not published on the manager web site.

**Allow external attendees**: defines a public conference and indicates that the conference location is accessible to any user navigating to the conference URL.

**Allow external attendees, with password**: defines a public conference and indicates that the conference location is accessible to any user navigating to the URL and can correctly supply the defined password. This password is also made available to the associated conference technology providers for this conference and may be used to further limit participation in the online conference.

**Deny external attendees**: defines a private conference and indicates that only the attendees that can be identified as having been included in the conference invitation can be given the conference access pages. Under a configuration setting on a per-technology provider basis, this check can be deferred from the Conference Manager to the technology provider. If any provider associated with a resource defines that the Conference Manager should apply this check, then the Conference Manager will challenge each user accessing the conference location and confirm their credentials against those of the conference invitees before providing the conference access pages. This authentication challenge is configured by default on the *conferencingprivate* virtual root on IIS for Windows and basic authentication. As such, only conference invitees that have credentials known to IIS have access to the conference pages. The Exchange CTPs for data and video disable this selection by default to allow participation from users without windows credentials and defers access control to the data provider that uses public certificate authentication.

Since all conferences are accessed via these IIS virtual roots, any IIS defined restrictions can be globally placed on conferences scheduled against the resources associated the Conference Manager. This can be useful to limit participation of conference to specific class of user, for example, based on Windows domain accounts.

# Participation in a conference

The features and functions of the associated conference technology provider define access to participate in an online conference.

**The Exchange Data Conferencing Technology Provider** uses the NetMeeting 3.0 feature of public certificate authentication to identify a user as an invitee of the conference. When the organizer schedules a private conference, the CMS communicates this to the DCS and the conference on the T.120 MCU is secured.

When a user receives the conference access pages, they are given the information to call the T.120 MCU hosting the conference. In addition, they are supplied with a list of certificate authorities (CA) for which the data provider will authenticate users. The conference access page then communicates with the NetMeeting SDK to select a matching client certificate prior to initiating the call to the MCU. To the user, this process is seamless and the one-click join is available for both public and private conferences.

To host a private conference, each MCU must hold a machine authentication certificate from which it can authenticate with connecting NetMeeting clients. At service installation and periodically thereafter, should a failure occur, each MCU will automatically request from its Windows 2000 domain a machine certificate from any installed Certificate Server. Failure to find this server and retrieve a certificate will result in the DCS being unable to host private conferences.

Exchange will inspect either the email or the common name fields in the certificate to confirm the associated user has access to the conference.

For all private data conferences, all transmitted data is encrypted using the SSL security layer available with the Microsoft Internet Explorer 4.01 and higher.

**The Exchange Audio and Video Conferencing Technology Provider** provides no conference participation access control. The conference payload, the audio and video streams are also not encrypted and as such can be intercepted while being transmitted on the network.

To secure a videoconference hosted conference it is necessary to secure the network on which the data is transmitted.

Limiting the network IP addresses used for a conference can also control the scope of the conference. The scope defined by the conference IP address and time-to-live (TTL) can be selected by assigning specific scope selections to the Conference Resource. The network routers can be configured for the scope's limited address range so that the conference is only available on specific sub-networks.

The Exchange videoconferencing client also limits conference participation to users that have multicast connectivity to the network in which the CMS is residing. A resource property also can be set to enable clients without multicast connectivity or with a client machine unable to participate in a multicast conference to connect to the conference using a H.323 unicast call using NetMeeting.

# Administration

Administration of the Exchange 2000 Conferencing Server is integrated into Exchange 2000 Server administration and its use of the Windows Active Directory. The same administrative security groups can be applied to administration of the conferencing server.

## Windows site-based service

Unlike the server-based services provided by the Exchange 2000 server with mailboxes existing on a specific machine, the Conference Server is an abstract Windows Site-based service. The Conferencing Server is implemented by a number of interrelated services.

The CMS defines the top-level of the Conferencing Server's installation. Each CMS is installed into the Windows 2000 Site in which its machine is a member. Only one CMS is active within a site. Any additionally installed CMSs in a site will idle without processing any conferencing load and serve as a backup Host Server for the Conferencing Site. The configured Host Server defines which server is active; this defaults to the first CMS installed.

Conference Resources are created associated with a specific Conference Manager and hence a site. Any organizer with adequate permissions can reserve on-line conferences against any resource. All conference participants will access the conference using the Conference Access Pages at the configured web address. This address is also used to list all conferences scheduled at this location.

CTPs are installed onto each machine configured as a Conference Manager. Some providers however will use additional machines, such as the T.120 MCU whose network location may be within or outside of the associated Windows 2000 Site.

To configure the Conferencing Server at a specific location, it is necessary to access the **Conferencing** node from the Exchange System Management Console. Select the **Manage…** command then choose the name of the Windows Site in which the Conference Manager is installed. From there, the CMS, MCUs, resources and installed providers can be administered.

## Administration Groups

When installing the Conference Management Service, you are requested to define the Exchange Administration Group in which the service will be installed. These groups allow administrative permissions to be assigned to different users who hence receive control over different servers or services. Once a CMS from a specific Windows 2000 Site is installed into an administration group, all conference managers installed into that site are placed automatically into the same administration group. The servers from a specific site can therefore always be managed from a single administration group.

Since Conference Technology Providers are installed into specific CMS installations, the associated administration group also secures their administration.

# Service Management

Each service installed as part of the Conferencing Server can be controlled from either within the Conferencing Server management console, or through Windows 2000 server manipulation utilities. For users to change the state of a service, they require the associated Windows permission on that machine.

# Logging reports

The CMS can emit a report log for a number of high-level operations. The configuration to enable these events is defined on the CMS property page. Each reported event is written to a comma delimited text file that is named dependent on the day on which it was generated. These files are automatically purged after the same duration as is defined for Exchange 2000 message log files.

These files can be found in the exchange logs directory, typically:

\exchsrvr\<server>.log\conferencing.log\yyyymmddCMS.log

Conference Technology Providers may also provide event logs that may be found in the same location.

These files can provide the administrator with the ability to analyze the operation of their Conferencing Server, for example, for billing or usage analyses. For instance, if a large number of users are found to be scheduling online conferences against resources at one specific location, this may be an indicator that an additional conference manager and associated resources should be deployed closer to their geographic location.

# Client Overview

## Requirements to participate in a conference

Components within the Conferencing Server have client requirements dependent on the features it provides and level of functionality available to the client.

> Note: The best user experience is achieved from a client using Outlook 2000 on Microsoft Windows 2000, including Internet Explorer 5.0 and NetMeeting 3.01 on an IP-multicast enabled network

### Conference Management Service

The CMS is responsible for processing the scheduling of online conference and for providing users with access to the conferences.

A conference can be scheduled in one of the following ways

- **Direct booking**: Outlook 2000, or newer, is enabled to directly book, i.e. confirmed reservation, Conference Resources. Users cannot book online conferences in the same manner when offline or disconnected from their Exchange server. The link to access the online conferences is automatically included in the conference invitation sent to all attendees.
- **Asynchronous email Request**: Outlook 97, Outlook 98 or Outlook 2000 or newer can send a conference invitation to a conference resource. The CMS will send a conference accept message, assuming resources are available, for the conference invite including a link to access the online conference.

To join a conference, the attendee requires a JavaScript enabled, frames capable browser such as Internet Explorer 4.01 or Netscape 4.5 or newer. However, to subsequently participate in the online conference, the client requirements are dependent on the conferencing technology associated with the conference technology provider. The following section describes the client requirements for the providers supplied in Exchange 2000 server

### Data conferencing provider

The DCS requires the client machine to have installed a T.120 compliant application such as Microsoft NetMeeting. The DCS directly supports NetMeeting versions 2.0, 2.1x 3.0, 3.0x with increasing levels of functionality. With versions prior to 3.01, the DCS will automatically run NetMeeting when the client accesses the online conference and connect it into the associated T.120 conference. NetMeeting will be run as a top-level application. Starting with NetMeeting 3.01, the DCS will, in addition, host NetMeeting's data collaboration controls directly within the conference web page, given the Internet browser supports ActiveX controls. Running NetMeeting 3.01 or above will enable the client to participate in DCS secure conferences by automatically selecting a client installed public certificate and after authentication, will subsequently encrypt their connection into the associated T.120 conference.

On platforms, or machines without NetMeeting installed, the DCS will request the user to start their T.120 client and accept the subsequent invitation it will send from the associated T.120 conference.

Participation in an access-controlled conference is only supported from a client using Microsoft Internet Explorer and NetMeeting 3.01 or above.

## Video conferencing provider

The experience of a user accessing a videoconference is defined by the client's platform and installed application software.

Clients accessing an online conference from a client installed with TAPI 3.0 or higher, such as Microsoft Windows 2000 and running on an IP-multicast enabled network will receive a multi-party, continuous presence representation of the videoconference participants. These participant video images are embedded into the conference web page using an ActiveX control. See the online help for more information about the video client.

As the administrator, you can also enable access to videoconferences to clients on platforms without TAPI 3.0 or a multicast enabled network by ensuring a version of greater than NetMeeting 2.1 is installed on the client machine. If available, the VCS will connect these users into the videoconference using a H.323 unicast NetMeeting call that it bridges into the IP-multicast videoconference. Users that connect in this manner will receive a full five participant mix from the audio of the conference and a single video image of the current participant speaking in the conference.

## 3rd Party Conference Provider

The client requirements to participate in a conference scheduled using a third party provider is defined by the requirements of that provider.

# Outlook 2000 integration and configuration

Available to users with Outlook 2000 or newer, is the ability to use Outlook's direct-booking feature to achieve confirmed reservation of Conference Resources as an integral part of scheduling an online-conference. To enable this feature in Outlook 2000, it is necessary for a registry key to be set on the client's machine as described in the following procedure:

**Configuring Outlook 2000 enable confirmed reservation of online conferences**

- Note: This procedure is in the online documentation.
- Complete the following steps to enable Outlook 2000 users to schedule online conferences with the Conferencing Server, and to add the "Join Conference" button and menu item to Outlook 2000.

1. Using Notepad, create a file that contains the following text:

```
REGEDIT4
[HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Outlook\ExchangeConferencing]
```

2. Save the file, and give it a name with a *.reg extension. For example, name the file ConfSvc.reg.
3. Distribute the file to any Outlook 2000 user who will be scheduling or participating in online conferences.

Instruct the users to double-click the file.

> Note:
>
> This registry key can be defined using the Outlook deployment kit as part of your initial Outlook 2000 deployment or via a user policy regime such as can be achieved using Microsoft SMS or Windows network logon scripts.

## Optional manual install of client component

To participate optimally in an online conference, each client requires certain components installed on their machine. Typically, these components are automatically downloaded and installed on the client when the user joins their first online conference. However, in some situations this auto-download of components is disabled due to company policy.

Therefore, for the users in such an organization to participate in an online conference, it is necessary to manually install these components.

The best way to manually install the ActiveX components is to prepare a logon script that copies the controls (CAB files), expands them in an application directory and registers them on client machine. There are two files to copy: Xcliacc.cab and Xipcctl.cab. The path for the cabinet files on your ECS server is ..\Exchsrvr\ Conferencing\<local dir>, where <local dir> is the acronym for one of the languages supported by the Exchange 2000, for example: USA or GER. Expanding the CAB files is performed through ‘Expand’ and registering through ‘regsvr32’ OS commands.

In order to enable automatic download of the control, make sure the following settings are configured for the Internet Explorer on the client machines.

In the IE custom security settings for Intranet/Internet (depending on ECS location) “Run ActiveX controls and plug-ins” must be enabled or at least set to prompt in order to allow proper operation.
”Allow per-session cookies (not stored)” must be enabled or set to prompt (either works and no prompt is ever displayed) for the conference panel to load properly—due to use of the conference profile that was created by the default.asp.

With security level set to medium (default for internet), there is no problem. If the default level is set to high and then customized so that “Run ActiveX controls and plug-ins” is set to prompt and “Allow per-session cookies (not stored)” is set to prompt, we will work properly if the user has previously installed the ActiveX controls. If they haven’t, “Download signed ActiveX controls” must be set to at least prompt.

# Deployment Overview

The following section provides an overview of the tasks necessary for deploying the Exchange Conferencing Server within your organization. Each task is explained in more detail later in the section

1. **Plan the conferencing topology that suits your organization.** Determine where to install Conferencing Server components. Initially, you may consider

installing all components on one server as a pilot deployment. Aspects of the conferencing topology include:

**Note** Throughout this document, 'site' refers to a Windows 2000 site.

- Determine where, on your network, you want to install Conference Management Service.
- Determine which conferencing technology your organization needs, for example Exchange Data conferencing or Video conferencing, or both. Will you require any additional technologies from third party vendors?
- Determine the number and placement of your T.120 Multi-point Control Units. How will you accept remote or Internet connections if you plan to have inter-site and Internet participants in your data conferences? Do you have any secure sites within your organization?
- What levels of integration will the Conferencing Server have in your existing Exchange organization?
- Determine where you want to locate the conference profile store, that is, the Conference Calendar Mailbox. (Put it on the same server as Conference Management Service for better performance.) You may want to make it a separate, private MDB for effective backup and restore.
- What naming and structure will you create for your Conference Resources?
- Where will the MADCAP services be installed?
- Will you need to configure any network routers for IP-multicast?

# Installation Overview

The Conferencing Server requires the deployment of at least one Exchange 2000 Server in your organization prior to installation. The Exchange 2000 Server can be installed at the same machine as the Conference Management Service.

For a minimum, feature complete installation of the Exchange 2000 Conferencing Server, the following components must be installed or available within your organization:

- Exchange 2000 Server in which the conferencing services will be integrated. This will include the requirement of having Active Directory Service installed.
- MADCAP service to arbitrate the allocation of IP-multicast address for videoconferencing. MADCAP needs to be configured with scope leases consistent with the configuration of videoconference Resources. MADCAP is a part of the Windows 2000 DHCP service configuration. For help with configuring your MADCAP service, see "Video Conference Planning and Configuration" later in this chapter
- Windows 2000 Server (or Advanced Server to support clustering) on which to install the components of the Conferencing Server
- The Exchange Conference Management Service installed into the Exchange 2000 organization to manage the reservation of conference resources and client access to online conferences
- The Exchange T.120 Multi-point Control Unit service to host the DCS conferences

- Windows 2000 Enterprise Root Certificate Authority or trusted Subordinate Root CA installed in the domain to enable private DCS conferencing
- Exchange Conferencing Server Administration tools to allow the configuration of resources and the conference service components
- Microsoft Internet Information Service to host the ECS conference access web pages.

    - The following procedure installs CMS, DCS, and the T.120 MCU Conferencing server software. VCS is installed wherever you install Conference Management Service.

    - **To install Conferencing Server**

1. Log on to a Window 2000 server using an account that has sufficient rights.
2. Start Exchange Server Setup.
3. In the **Component Selection** screen, click each of the following components, and then click **Install**.
    - **Microsoft Exchange Conferencing Manager Services (includes VCS)**
    - **Microsoft Exchange T.120 (MCU) Services**
    - **Microsoft Exchange System Management Tools**
2. Determine where you want to locate IIS. IIS hosts the conference access pages and must be present in each site where Conferencing Management Service is installed
3. **(Optional) Choose a fail over strategy.** Decide whether you want to set up a standby server running Conference Management Service or a clustered pair of servers using Microsoft Cluster Service.
4. **Plan the conference resources.** Determine the number and type of resources your organization needs, where they should be located, and their properties (such as *size* for DCS or VCS resources). Establish a naming convention for the resources.
5. (Optional) If you need to support secure data conferences, install Microsoft Certificate Services on at least one server in the domain.
6. **Install Conferencing Server components.** These include CMS, DCS, T.120 MCU servers, and any third-party conference technology providers.
7. **Configure the conference calendar mailbox.** For more information, refer to the Exchange 2000 Server online documentation.
8. **Create and configure the conference resources.** Assign the technology providers, and define the provider properties. For more information, refer to the Exchange 2000 Server online documentation.
9. (Optional) Install additional T.120 MCU Conferencing servers in the domain and configure their “scope,” or network visibility
10. **Notify users about Conferencing Server.** Tell your users that the service is available, which client applications they need to participate in the different types of conferences, and where to get the clients.
11. **Enable Outlook 2000 Users for Direct-Booking of Conference Resource.** As part of deploying the Conferencing Server to users, you must create a strategy

for enabling Outlook 2000 users with the necessary client registry file configuration modification.

# Best Practices

The following are the strategies and practices that we would recommend to follow when planning your Conferencing Server deployment:

- If you plan to hold conferences with anyone outside your organization (for example, on the Internet), you should initially consider placing the IIS service on an independent computer whose DNS host name can be resolved by both internal and, eventually, external clients.
- Make conference resources and the conference calendar mailbox the only mailboxes on the server running the Conference Management Service. If, however, you must share the server with user accounts, put the conference resources and the conference calendar mailbox in a separate MDB. Applying this strategy will minimize downtime if you need to restore scheduled conferences or move them to another MDB.
- Keep the conference calendar mailboxes on the server with the active Conference Management Service. Performance may dramatically decrease if they are on different servers.
- Use descriptive names that distinguish your conference resources from physical meeting rooms. For example, you can use **“Virtual team-conference(10)** for the display name of a data and video conference resource with a size of 10. Define multiple resources of the same type in different sizes for more efficient use of resources.
- If you have multiple conferencing sites, use resource names describing their location
- If your site has multiple subnets with slower links among them, consider placing one or more T.120 MCUs on each subnet; configure the MCUs to accept connections only from the users of that subnet.
- Even if you are going to initially run the IIS server on the same, default, machine as the CMS, change the meeting access location address to a virtual name for that machine. This way, users will not lose access to the scheduled conferences if you decide to move IIS to a separate machine at some point. You will only need to change the mapping on the DNS server to point the virtual name to the new IIS server.

If you are new to online conferencing and are deploying Conferencing Server for the first time, consider a phased rollout. Deploy the service on one server and give access to a single group. Then, add additional servers and groups based on increasing demands for the service or specific usage patterns (for example, concentrations of users in remote areas).

# Conference Management Service

## What is the Conference Management Service?

The Exchange Conference Management Service (CMS) is the component of Exchange 2000 Conferencing Server that is responsible for the management of Conference Resources and support of Conference Technology Providers. The CMS runs as a Windows 2000 service on a specific Conferencing Server. Only one server, known as the Host Server, actively runs the task of conference management within a Window 2000 site. Multiple such servers can be installed. Using the Conferencing Server administration, the currently active Host Server is selected.

The service facilitates the arbitration between scheduling of Conference Resources and the subsequent reservations held in the Conference Calendar Mailbox. The service provides the facilities to the providers to publish resource availability in the Exchange free/busy store and the implementation of confirmed reservation via Direct Booking. The CMS also controls the lifetime of online conferences and provides support for conference deletes and modifications.

All conference attendees interact with the CMS and the associated Conference Access Pages to request participation in a specific online conference. Dependent on configuration, the CMS also implements conference access control through client authentication.

A user interacts with the Conference Manager in two ways, scheduling a conference, and joining a conference. The following sections describe the basic theory of operation for these two activities.

## Scheduling a conference:

All conferences are scheduled by initiating a conference reservation request inviting one of Conference Resources. Conference requests arrive through one of two ways, a confirmed reservation through Outlook direct booking, or asynchronously through a received email request. Assuming the associated conference technology providers accept the conference request, the CMS stores the details for the conference in the Conference Calendar Mailbox. This persistent representation for the online conference also offers the providers a storage location for information associated with the conference, such as an archive location for a conference recording.

The CMS maintains the accuracy of the conference definition by processing all conference updates and publishing of associated free/busy data.

When the conference is due to start, the CMS notifies all relevant technology providers and defines the conference as in-session. When a user requests to attend the conference, the CMS negotiates with the technology providers the information required to attend the conference.

## Joining a conference:

Join Scenario: A user requests to attend an online conference by opening the location specified by the conference URL.

The CMS takes this user request and attempts to find the associated conference stored in the Conference Calendar Mailbox.  A user can request to join a conference before the scheduled time, during the scheduled time, or after the scheduled time. The CMS works with the technology providers to distinguish these three permutations and provides the user with different information. Joining a conference while in session would place the user directly in the associated conference. The specific users' experience when they join before, during or after the conference is dependent on the technology providers that were invited to the conference.

On locating the conference definition in the Conference Calendar Mailbox, the CMS will inspect the organizer requested level of access control, whether a password is required or if the CMS is required to authenticate the user before referencing the user to the CTP.  The CMS will then work with the technology providers to return the user the correct information.

While the participants are in conference, the CMS also permits the organizer to modify the end-time and properties of the conference.

# Deployment strategies

The Conference Management Service is deployed on one or more Conferencing Servers within your Exchange Organization. Only one CMS can be active per Windows 2000 site. This Conferencing Server running the active CMS is known as the Host Server. The Windows site in which a CMS is installed is known as a Conferencing Site.  The Conferencing Site defines a collection of Conference Resources and Conference Technology Providers associated with the CMS.  More than one CMS may be installed within a Conferencing Site, however any additional CMS will be inactive and not share the management load. These inactive management servers may be required as a backup to the active CMS in case of server failure.  Such backup conference management servers can become active automatically if deployed as part of a Windows Cluster, or manually from the Conferencing Server administration.

- One or more CTPs are installed into a Conferencing Site.  Some providers, such as the DCS, also include additional services such as the T.120 Multi-point control Unit.  These additional services may run on additional servers, however, at least the base implementation of the CTP code runs on the same server as the CMS.

- Only the conferences scheduled at a specific Conferencing Site are accessible by the Conference Access Pages hosted in that site.  The actual conferences may span multiple Conferencing Sites.

- Since all conference reservations and client requests are processed by the single CMS within a Conferencing Site, you must plan the server load that will be generated from the utilization of the service to match the capacity of the server running the CMS.

- The determination of how many and where you deploy Conferencing Sites within your organizing includes dependencies on the following aspects of your organization:

- **Anticipated schedule load**.  Since only a single CMS is active within a site, it may be prudent to balance your user load across multiple sites assigning users to the sites according to their geographic location. For example, install CMS within your distributed data centers that currently contain email services.

- **Logical separation of conferences**. For example, you may deploy a Conferencing Site with Conference Resources solely used for conferences needing to be published to the Internet or within some organizational boundary.
- **Multi-site conference topologies**. The DCS uses the Conferencing Site architecture to refer client join request to the T.120 MCU that is 'closest' to the user's machine.

Deployment of a server running a CMS and hence the associated creation of the Conferencing site can start safely from the deployment of a single pilot server.

You can upgrade the Conference Server either in anticipation of existing demand or by analysis of usage patterns. Existing demand may dictate additional Conferencing Sites due to obvious physical aspects in your company such as more than one existing data-center. For all the same reasons you may have placed the email servers for your organization within these data centers, you would place a CMS. If such demarcations are not so pronounced, then analysis of the CMS audit log files will show where the users that schedule conferences exist within your organization. If these logs show you have a lot of conferences at one location, then the installation of an additional Conferencing Site closer to their network location should ease the schedule load across your network and enable the DCS the ability to better create distributed conference topologies.

# Placement of Conference Technology Providers

Along with each Conference Management Service, a Conferencing Site has installed one or more Conference Technology Providers. The users to schedule reservation against these CTPs use the Conference Resources created in the Conferencing Site.

The ECS installs both the DCS and the VCS whenever you install the CMS. You can however select which CTP you create resources for and hence which providers are active within a specific Conferencing Site. Also, any additional third party providers are installed after the CMS and can be installed only into the Conference Site in which you want resources of that type. For example, if you made the deployment decision to build a separate Conferencing Site for online conference with Internet attendees, you may prefer only to create DCS Resources since typically videoconferencing would not be widely used over the Internet.

# Conference Access via IIS

By default, Conferencing Server uses the Conference Access Pages running on the IIS installed on the CMS Host Server.

The location of the conference pages are indicated by the conference access URL and takes the following general form:

`http://<server_name>/conferencing`

This URL is the base address of the IIS server that hosts the conference access pages for the Conferencing Site. It is displayed on the **Conference Settings** tab in the Conferencing Server site properties.

If you plan to host the conference access pages on the same server on which you install the CMS, you do not need to change the default conference access URL. However, if you want to change the URL to refer to another location, you must also make the following configuration changes in the Internet Services Manager snap-in:

If you change the conference access URL to refer to a different server, you must first install the CMS on that server, and then, either redirect client requests for previously scheduled conferences to the URL on the new IIS host server or change the DNS server settings to point to the new IIS server.

# Defining the default conference access location

It is highly recommended you use a logical server name for the machine hosting the Conference Access Pages, even if this is to be hosted on the default Conference Management Service server. This machine name will be embedded in all scheduled conferences. If you accept the default WINS network address, then this address must always be used. This limits your ability to grow your deployment by placing the Conference Access Pages onto their own server or by using some load-balancing technology such as DNS round robin or Windows Load Balancing to spread the load across multiple servers. Such a configuration could be accomplished by adding a logical DNS name for the hosting machine and changing the client access location to use this name.

# Scalability

A single Conferencing Site through the Conference Access Pages installed on the default Host Server can service the demands of most companies. However, in very large organizations or companies that place a big demand on their Conferencing Server, and it may be necessary to dedicate a machine to processing conference access request, or in some case share this load across multiple machines.

Depending on your network bandwidth, server power and ECS usage a single CMS server is capable of maintaining from thousands to hundreds of thousands users in a site. However, if the network is segmented and geographically dispersed with low bandwidth links between the remote locations, it is advised to define a separate Windows 2000 site in each of such network segments and deploy ECS in each site where conferencing services are expected to be used regularly. Such configuration can scale to support any existing organizational conferencing needs.

# Reliability Planning

To deploy a highly available Conferencing Server it is necessary to define a reliability plan. This plan will define the level of redundancy and policy action in the result of any component failure. To define this plan, it is necessary to understand the points of possible failure within a Conferencing Server deployment and the options available to ensure some form of fail-over strategy.

The following table highlights the major area of possible failure within a Conferencing Server deployment and the options and strategies you can take to ensure the service will continue to be available

| Component | Type of Failure | Recovery or fail-over options |
|---|---|---|
| Conference Calendar Mailbox | Disk failure | • Place data on a redundant RAID array.<br>• Place mailbox in separate storage group and backup frequently |
| Conference Calendar Mailbox | Exchange Server | • Put the Exchange Server into a Active/Active cluster |
| CMS | Server/ Service | • Put Conference Manager into a Active/Passive cluster<br>• Ensure you have a backup CMS installed to allow you reconfigure the service onto the backup machine |
| Conference Access Pages | Server/ Service | • Use Windows load-balancing for the IIS service<br>• Have conference access pages installed on a spare server, change configured DNS address of the Conference Location to the backup server |
| T.120 Multi-point Control Unit | Server/ Service/ Network | • Ensure each Conferencing Site has multiple servers that can accept client connections for the same user locations. |
| MADCAP Service | Server/ Service/ Network | • Install more than one MADCAP server and select scopes on the conferencing resources from both servers. |

# Backup/Restore strategy

The Conferencing Server places or uses configuration and service data in the following locations:

**Exchange Server**: Including the Conference Calendar Mailbox and Conferencing Resources

**Windows Active Directory**: Includes all service configurations.

**MADCAP Scopes**: The definitions of scopes defined by the MADCAP services are referenced from the Conferencing Resources.

To recover from catastrophic failure, it is therefore necessary to follow the backup/restore strategies for each of these components.  A description of these strategies can be found in the Exchange Server and Windows 2000 documentation.

# Conference Management Security Model

## Public and Private Conferences

When the organizer of an online conference creates the schedule request, they have the ability to specify whether their conference is open to the public or is private, i.e. accessible to only the invited participants. The Outlook 2000 calendar setting, “Allow external attendees”, identifies a public conference. If they select a public conference, they have the option to specify a password that will be required to access the conference. Anyone that is invited to the conference as part of the initial schedule request will automatically receive this password as part of the conference location URL. All public conferences are listed on a page accessible from the conference access page’s home page. The URL for the list of public conferences is http://<server_name>/conferencing/list.asp.

Online conferences scheduled using Outlook Web Access for Exchange 5.5, or versions of Outlook prior to Outlook 2000 can only schedule non-password protected, public conferences.

The type of the conference, whether it is public or private, or with a password is also communicated to the associated conference technology providers. The CTP may therefore also provide additional public/private semantics. For example, the DCS will force public certificate authentication and subsequent transmitted data encryption when it hosts a private conference.

## Conference Access Control

The concept of a private conference is to indicate the desire to restrict the attendees of the conference to only participants that can be authenticated as invitees of the conference. The Conferencing Server administrator can configure the level at which the control over who can access a conference is provided. Each ECS CTP indicates to the CMS its desire for the conference access pages to assert a conferences access control. This setting is configured via the “Authenticate access to private meeting pages” setting on the CTP property page. When any provider of an online conference has this enabled, the CMS’s conference access pages will force the user to an IIS virtual directory that requests for user authentication. The user must be an invitee to the conference to be allowed to attempt to join the conference. The ECS CTPs by default do not require this setting to allow online conference attendee from outside of the organization.

If a password-protected public conference is created, the password must be provided at the conference access pages to allow entry into the conference. Direct invitees of the conference will receive this password attached to the conference URL allowing direct entry, however any user attempting to join the conference from the conference listings will be required to know the password by some other means.

## Security Supplied by CTP

Each CTP involved in the online conference is informed of the security level of the scheduled conference. The level at which the provider will secure the information within their conference is dependent on the technology.

The DCS will allow any user access to a public conference. Since access to the conference is through the conference access pages, the T.120 protocol level publishing or listing of a conference by the MCU is disabled. For password-protected public conferences, the password is also required to be specified within the T.120 protocol for access to the conference. For a private conference, a public certificate must the exchanged with the MCU that authenticates the user as an invitee of the conference. In addition, the connection between the user and the MCU, and any other MCU in the conference is secured using Secure Socket Layer (SSL) encryption.

The VCS does not distinguish between public and private conferences.

# Resource Management

Each CMS within a Conferencing Server deployment manages a set of Conferencing Resources created to represent the physical resources provided by the associated installed conference technology providers.

Each CTP will typically differ in what it describes as its physical resource. For example, the DCS uses the concept of a user connection to an MCU as the consumable unit of resource. The VCS uses a concept of a stream of audio-video as the consumable unit of a resource; a telephone provider may use a port on a PBX or the processing power of a digital signal process.

To support these many varied forms of resources, the Conferencing Server defines an abstract resource model and a simple associated rule of availability. Each CTP, when installed on a Conferencing Server, describes the availability of its physical resource and its ability to be integrated into the abstract resource model.

Grouping the definition of one or more provider’s physical resources and their associated properties creates a Conferencing Resource. The combination of providers and the physical resource’s properties as defined on the Conferencing Resource, specify the experience the attendees of a conference will enjoy when participating in a conference scheduled with that Conferencing Resource.

# Defining the conferencing experience

The user experience for the participants of an online conference is defined by what combination of providers and properties are set on the conference’s Conferencing Resource. The Conferencing Server administrator creates the Conferencing Resources and defines the associated provider properties. The selection of what combinations they create is defined by what facilities they want to offer the users of the service. For example, it may be that the company network simply cannot support videoconferencing; therefore, the Conferencing Resources are created using just the DCS. With the availability of third party

providers, additional resources may be created to offer, for example, a simultaneous telephone and data conference.

In addition to the basic conferencing experience, the Conferencing Resource's CTP properties can also affect the user experience. For example, say the decision was made not to place video on the company network; the VCS can instead be configured to only support the audio part of the conference in the conference. Defining the property that selects which CODEC is used for the audio defines the quality and bandwidth used by participants of the associated online conference.

# Naming Conventions

Since each Conferencing Resource is published in the Exchange address list, it is important to define a convention to name and describe the experience and capability of the resource.

The following aspects of a resource effect how the names for resources should be defined:

- Are there multiple Conference Management Services within the organization that publish resources specific to their Conferencing Site?
- What form of user experience or scenario do the resources address?
- Are there any specific aspects of the resource that would affect which resource an organizer would select for their conference, such as the size?
- Are any resources restricted in who has permission to reserve it?

All Conferencing Resources from all Conferencing Sites can be listed from within Outlook's address form by selecting the "All Conferencing Resources" address book view. Within an Exchange 2000 Server it is possible to create additional address book views that group both mailbox users and resources into additional address lists. These address book views can be used to group the resource mailboxes used for conferencing.

The following examples of resource naming may be suitable for your organization:

- **Location based scenario**: Using aspects of the CTP's properties that limit participation of the online conference to some geographic region along with the target scenario and the size of the conference. For example:
  - Redmond virtual team conference (10)
  - Redmond videoconference (8)
  - New York teleconference (12)
- **Technology Based**: Exposing the technology that defines the resource can sometimes be most informative to the organizer. For example:
  - Online data/video (10)
  - Online video [CIF] (4)
  - Online telephone/data (12)

In each case, the size that indicates the maximum number of participants is displayed in much the same way a physical meeting room often displays the number of people the room can seat.

# Configuring Resources

Only a single Conference Resource of a specific configuration needs to be created. For example, only a single Conference Resource that represents a data conference for 10 people needs be created. Unlike the address book entry that is created for a physical meeting room, the Conference Resource entry can be invited to conferences multiple times before it is considered busy. Resources are configured as properties of a Conference Management Service within a specific Conferencing Site. Only the CTPs installed in the Conferencing Site can be assigned to a Conferencing Resource.

Since all public conferences are listed on the Conference Access Pages for all conferences scheduled within a Conferencing Site, it may sometimes be prudent to limit the permissions to invite resources of a Conferencing Site that allows collaboration with participants from the Internet. For those 'Internet' resources, the name should be in some way distinguished to inform the conference organizer.

# When is a resource busy

Each Conferencing Resource publishes into the Exchange free/busy public folder its ability to accept additional reservation requests. Each CTP associated with the resource, independently computes its ability to accept additional conference invitations based on the cost associated with the resource and the currently accepted conference requests.

If any of the providers associated with a resource are unable to accept the additional schedule cost, then the resource will be indicated as busy.

To take an example, assume a Conferencing Server has two conference technology providers, the first, 'A', has a maximum resource availability of 50 units. The second, 'B', has a resource limit of 100 units.

Associated with these providers are the following resources:

A(10), B(10), A(40), A+B(20)

the resource unit costs are indicated in parentheses.

Initially all resources publish a free status. Assume a conference using resource A+B(20) is scheduled, the cost associated with the resource are decremented from both provider's total. At this point, 'A' would have 30 units available, 'B' 80. Since 'A' has now only 30 units available, the A(40) resource changes to publish busy. However, A(10) can still accept three reservations before it publishes busy.

# Conference Calendar Mailbox

The deployment of each Conference Site requires a Conference Calendar mailbox to be defined and assigned to the CMS. This must be done before any online conferences can be scheduled against resources associated with that Conferencing Site. To assign the Conference Calendar Mailbox, select 'manage' from the Conferencing Server administration tool and at first run, will prompt you through the process. For more information, see the online documentation.

For performance reasons, it is recommended to locate the Conference Calendar Mailbox on an Exchange Server as close a possible, preferably the same, to the

Conferencing Server hosting the CMS. In some deployments, both the Exchange Server and the CMS are run on the same machine.

The purpose of the Conference Calendar Mailbox is to create a store of all scheduled online conferences. Each online conference defines a single entry in the Conference Calendar Mailbox. This entry defines all the properties of the conference such as its security level and conference invitees. Some providers also use this conference item to store additional information associated with the online conference. For example, the VCS stores in the conference item the multicast description of the videoconference. A third party conference archive provider may use the conference item as the storage location for a recording of the conference.

Since the Conference Calendar Mailbox contains the definitions of all conference schedules within a Conferencing Site, it is critical this information is not lost and is available to the CMS at all times. As described earlier in this document, for reasons of recovery from a disaster, the Conference Calendar Mailbox is often placed in its own Exchange Storage Group to facilitate independent back up and restore processes and to serve as a unit of fail-over when installed in a cluster.

When applying storage limitation policies on the Exchange mailboxes, take care to ensure the Conference Calendar Mailbox always has enough storage to still hold the required number of online conference definitions.

Since all scheduled conferences within a Conferencing Site are stored in the Conference Calendar Mailbox, it is necessary to periodically either purge or archive historic conference definitions. An Outlook profile can be created to attach to the Conference Calendar Mailbox and either using Outlook's archive feature, or manually, items should be removed from the mailboxes calendar folder to prevent the mailbox exhausting available storage space.

# Conference Access Pages

Associated with each Conferencing Site's CMS is a web site that hosts the Conference Access Pages. All conference participants who attend an online conference access these pages. These pages also include a list of public conference that can be selected to attend the conference.

Since all conference participants are required to retrieve pages from this web site, the sites network address must be accessible by all users that need to attend the conferences. If this includes attendees from the Internet, then the Conference Access Pages must also be available to users from the Internet.

The network address of these pages is included in the conference access URL that is sent to conference invitees. It is important therefore, that this network name never changes; otherwise, all existing conference definitions will become invalidated. To accomplish this requirement, it is often simplest to define a virtual network name, normally using DNS, for the machine hosting the conference access pages. It will be necessary to modify the address defined by the Conference Management Service to use this virtual network name. For details, see the online documentation.

A single Internet Information Server will be sufficient, in most cases, for hosting all the users within a conferencing site. However, either for reasons of redundancy or deployment within very large organizations, it may be necessary to place the Conference Access Pages on more than one server. Each server should be addressed using the same virtual network name as configured on the

Conference Management Service.  This can be achieved either by a DNS round robin configuration or by deployment of IIS using a Window Load-Balancing setup.

IF your IIS server is expected to accept connection from Internet attendees, in the security settings for the ‘ConferencingPrivate’ virtual root in the default web site uncheck “Integrated Windows authentication” option. This will enable Internet users to participate in private conferences using basic authentication.

**Warning:**  remember that basic authentication sends user’s credentials, including the password, in plain text format.

# Deploying the Conference Management Service

The Conference Management Service is the service that, when installed into a Windows 2000 Site, creates the Conferencing Site. How many Conferencing Sites your organization requires and where they should be located, is dependent on the network topology and concentration of users wanting to schedule online conferences.

If the ECS is your first experience with an online conferencing solution, knowing where the user demand will originate can be difficult. Using the audit log files generated by the CMS, it is possible to initially deploy a single management service and monitor usage to analyze where and if additional Conferencing Sites are required.

For an initial or pilot deployment, it is possible to run all conferencing services on a single machine. Ensuring you created a virtual network address for the conference access pages, this pilot can grow into a full international, multi-site conferencing deployment.

Before a Conferencing Server can be installed, certain services must be already available within your organization's network.

- **Exchange 2000 Server:** An Exchange organization containing at least one Exchange 2000 Server is required before the Conferencing Server can be installed. The conferencing services can be installed either all on the same server as an Exchange Server or each on an additional machine. Exchange 2000 Server has a number of dependencies, such as Windows 2000 Active Directory that are also required by the Conferencing Server.
- **Windows 2000 Server:** The conferencing services must be installed on a Windows 2000 Server. If you need to cluster the management service, then this must be Windows 2000 Advanced Server to have the clustering support. Each component service of the Conferencing Server can be installed on either a dedicated machine or share a single machine for all services.
- **Windows 2000 MADCAP Service:** To support and configure the VCS, it is necessary to have deployed one or more MADCAP services. This service is installed by selecting the DHCP service from within the Windows 2000 Network components. It is possible however to run MADCAP on a machine without enabling DHCP services also. See Windows 2000 online documentation on how to install and configure MADCAP.
- **Windows 2000 Certificate Server:** To fully support the DCS, it is necessary to have deployed at least one Windows Certificate Server within the active directory forest that contains T.120 Multi-point Control Units. To support authenticated and encrypted private conferences, each MCU queries the Certificate server to retrieve a machine certificate for its own use and to validate client certificates when a user attempts to join a conference.

The first CMS to be installed into a Windows 2000 Site becomes the active Host Server for the newly created Conferencing Site. By default, both the DCS and VCS are installed along with the CMS. However, to support data conferences, it is necessary to also deploy at least one T.120 MCU.

Any additional installations of a CMS into a Conferencing Site will run in an idle state. Through the Conferencing Server administration, it is possible to move the Host Server so an idle server becomes active.

If a Windows2000 Cluster is to be created, the clustering deployment wizard is used to link two Conference Management Servers together to achieve an automatic fail over between an active, and idle server.

Before a Conferencing Site is able to host online conferences, it is necessary to assign the site's Conference Calendar Mailbox, install any additional services required by the conference technology providers, such as the Exchange T.120 MCU, and create the associated Conferencing Resources. For details on these configuration steps, see the Conferencing Server online documentation.

If your organization has more than one geographic concentration of users needing to schedule or join online conferences, you may want to consider the creation of additional Conferencing Sites. Since each Conferencing Site has its own Conference Calendar Mailbox, a set of Conferencing Resources and Conference Access Page's network address configurations will be needed for these additional sites.

The distributed nature of the components within a conferencing site offers great flexibility in the deployment of the Conferencing Server. By associating the definitions of Conferencing Resources with a specific CMS, the associated CTP resources and public conference lists can be separately managed. For example, creating a single Conferencing Site within your organization with connectivity to the Internet allows for only the conference schedule on its resources to be published and accessible from the Internet, however still permitting internal conferences to be scheduled.

**Note:** If you install the Conferencing Server primarily onto an Exchange 5.5 organization running on Windows NT 4.0 domains, and if you plan to deploy more than one Conferencing Site or data conferencing with connectivity to the Internet, in addition to configuring the Active Directory Connector (ADC) for account replication, you must configure the site subnet definitions from Windows 2000 Sites and Services administration. If no Windows 2000 sites are defined, then all users and all conferencing Servers will assume they belong to the local site (the only site) and none of the 'closest server' topology and inter-site referral will occur. If your organization requires only a single site definition, and for security reasons you don't want to expose your primary Exchange server to the Internet, a second site must still be defined to identify user connections originating from the Internet.

# Server Requirements

The Conferencing Server that hosts the CMS must be installed on a Windows 2000 Server. Windows 2000 Advanced Server is required for clustering.

This machine must be a member of the Windows 2000 domain in which the Exchange 2000 Server is a member. All Conference Calendar Mailbox and Conferencing Resources associated with the CMS must have the associated Windows account within that same domain. At least one Exchange Server within the domain must also include, or have a replica of, the organizations public folder for free/busy data.

Each server hosting the Conference Access Pages must be a member of the same Windows Site as the CMS server and be able to connect using DCOM/RPC.

The recommended requirements for CMS server hardware is:

400 MHz Pentium.

256 MB of RAM.

# Administration

All administration for each of the Conferencing Server services is achieved using the Conferencing Server Administration snap-in.  Each Conferencing Site deployed within the organization can be managed separately. Instructions on how to manage a Conferencing Site can be found in the online documentation.

Administration can be accomplished from any Windows 2000 machine that is a member of the Windows 2000 forest from a user account that has adequate access permissions.  The administration applications can be installed separately to any other conferencing service.  Administration from non-Windows 2000 clients can be achieved by installing Windows Terminal Server.

# Permissions

## Exchange Conferencing Management and Providers

To manage and configure site-wide conference settings, CMS, DCS, and all T.120 MCU servers, you must be a member of the Exchange administration security group within the domain in which the Conference Server is configured.

## Conferencing Server Services

To alter the running state of a service, such as the CMS or T.120 MCU, you must have rights to stop and start services on those machines.

## Resource Management

To install the ECS components, to create and manage the conference calendar mailbox and any conference resources, you must have sufficient permissions to create domain user accounts.

# Exchange Data Conferencing Service

Included in Exchange 2000 Conferencing Server is a conference technology provider for data conferencing.  Unlike existing solutions for data conferencing, the DCS includes both the T.120 MCU of a typical conferencing solution but also the generalized resource model, integration into the CMS and MCU fail-over,load balancing and topology control logic.

# What is Data Conferencing?

Microsoft NetMeeting and its ability to share applications and data between multiple machines simultaneously made data conferencing popular. A data conference has the following features:

- **Application sharing.** You can share a program running on one computer with other participants in the conference. Participants can review the same data or information, and see the actions as the person sharing the application works on the program (for example, editing content or scrolling through information.) Participants can share Windows-based applications transparently without any special knowledge of the application's capabilities.

  The person sharing the application can choose to collaborate with other people in a call, and all the participants can take turns editing or controlling the application. Only the person sharing the program needs to have the application installed on his or her computer.

- **Shared clipboard.** The shared clipboard enables you to exchange its contents with other people using familiar cut, copy, and paste operations. For example, you can copy information from a local document and paste the contents into a shared application as part of group collaboration. This capability provides seamless exchange of information between shared applications and local applications.

- **File transfer.** With file transfer capability, you can send a file in the background to one or all of the people in the current call. You can right-click on a person and choose to send them a file, or you can drag a file into the Microsoft NetMeeting window and have the file automatically sent to each person, who can then accept or decline receipt. The file transfer occurs in the background as everyone continues sharing an application, using the whiteboard, or chatting.

- **Whiteboard.** The whiteboard is a multi-page, multi-user drawing application that enables you to load or sketch diagrams, organization charts, or display other graphic information. Whiteboard is object-oriented (versus pixel-oriented), allowing you to move and manipulate the contents by clicking and dragging with the mouse. In addition, you can use a remote pointer or highlighting tool to point out specific contents or sections of shared pages. This capability extends the application-sharing feature of NetMeeting by supporting spontaneous collaboration on a common drawing surface.

- **Chat.** You can type text messages to share common ideas or topics with other people, or record conference notes and action items as part of a collaborative process. You can also use Chat to communicate in the absence

of audio support. The NetMeeting “whisper” feature allows you to have a separate, private conversation with one of the conference participants during a group chat session. From the Chat window, click on the person’s name in the ‘Send To’ list, and type your private text message that only you and the selected person will see.

NetMeeting 3.01 or higher is the recommended client software for Exchange DCS. It provides all the above-mentioned features, is capable to run as an embedded control in the web page and facilitates private, secure conferences.

# Joining a data conference

Every online conference is identified by a conference access URL. All participants of a conference scheduled against any combination of conference technology providers use the same URL. The following is a description of what happens on the Conference Server to support a users access to a data conference.

With respect to the scheduled time of the online conference, a user can access the URL at some time before the conferences start time, some time after the conferences end time, or while the conference is in session.

The DCS supports all three levels of the ECS security. The public conference is open to participation from any user, the public conference with a password requires the user to enter the password to join the conference and the private conference requires the user to present a public certificate that correct authenticates them as an invitee of the conference.

Users that access the conference prior to the scheduled start time are told the conference has not yet started. If they stay on this page then they will automatically be joined to the conference when it starts. A user that accesses the conference after the scheduled end time is simply informed the conference is over.

When the users access the conference URL while the conference is in session, assuming they have access through the ECS security levels, they will be directed to a specific T.120 MCU dependent on the network address of the client accessing the conference. This client address is retrieved from the web browser and it is therefore important for an optimal topology creation that users within a Conferencing Site are configured to bypass any proxy server to access the Conference Access Page server. Users from a remote Conferencing Sites can successfully use an inter-site proxy as long as their proxy is identified as being within the remote Windows 2000 Site and within their site the user accesses their Conference Access Pages as local.

Using the clients IP address, the DCS inspects the current Conferencing Site deployments within the organization. If it finds a Conferencing Site that has preferred ownership of the user’s location then it will redirect the join request to the local Conferencing Site, supplying the network name and the conference name of a local T.120 MCU on which the two Conferencing Sites can be linked. Within the remote Conferencing Site, the DCS will select the best MCU in its site in which to attach the user to the conference.

If the user is accessing the data conference from a Windows client running Internet Explorer and NetMeeting, they will be scripted directly to connect to the MCU hosting the associated conference. If the user does not have any of those, a T.120 invitation is initiated from the MCU to the client’s IP address inviting them to the conference. If this invitation fails, the details for the conference are

displayed in the web page allowing the user to manually call into the T.120 conference.

# What is an MCU?

To create a multi-participant data conference it is necessary to involve a software component known as a multi-point control unit (MCU). This component is capable of interconnecting the network connections from multiple conference participants, and synchronizing and distributing the data in the conference between each participant.

The Microsoft NetMeeting client includes such a multipoint component embedded with it. This allows NetMeeting, at a peer-to-peer level, to support multi-participant data conferencing. Since each client connection to an MCU requires a separate copy of the conference data to be transmitted, a NetMeeting application with ten other peers would require that client to send ten copies of the information. If that user is on a modem or at the other end of some slow WAN link, it quickly becomes apparent that this is not the most efficient solution.

Moving the MCU component onto a central server and allow each participant to connect to it, does solve the issue of a client needing to send multiple copies of the conference information. Deploy this MCU server in a manner that bridges multiple networks, then the conference can be held between participants on the Intranet and Internet at the same time. Additionally, when the conference is hosted on a server, the organizer, who typically is also the conference host, is no longer required to stay in the conference for the whole duration. In the peer-to-peer case, if the organizer needed to leave the conference, the whole conference would be dissolved and therefore the organizer must stay in the conference for the duration.

This single server deployment does not however address the issue of multiple participants on the remote end of a WAN link because it still requires multiple copies of the conference data to be transmitted across the link. What is required here is to put an MCU at both ends of the WAN link and instruct participants to connect to the MCU closest to the physical network location. Although increasing the complexity of participation in a conference, building a conference topology in this manner is possible even with peer-to-peer logic only. Stretch the conference over multiple WAN links with multiple participants that often travel, and change which MCU is closest and this manual solution quickly becomes impossible to manage. The DCS offers a solution to all these problems, creating an automatic topology that sends single instances of data across the WAN link. A persistent location for the conference allows all participants to come and go as required. It automatically directs a client to the closest server and, in addition, provides levels of security that ensure you know who you are in conference with and that no other users can listen-in on your conference.

# Resource Properties Settings

The DCS has a very simple resource model. An administratively set limit is defined of the maximum number of simultaneous client connections permitted across all T.120 MCU installed in the Conferencing Site. Each Conferencing Resource representing the data provider then has a size property that is used to define the number of participants allowed access to a conference scheduled using the resource. The size associated with the resource is then decremented from the maximum number of connections available for the period defined by the conference schedule. If the summation of the sizes associated with all conferences scheduled for some specific time period reaches the defined

maximum, then the provider resources go busy, and no additional data conference schedules are accepted.

# Data Server Deployment Topology

How you deploy your DCS depends on the topology and other characteristics of your network. It also depends on how you prioritize the different properties of the Conferencing Server. For example, is it important to localize on your network the traffic associated with a conference? Do you consider the cost of conference traffic across the network infrastructure higher than the management of additional decentralized servers?

The optimal number and placement of MCUs you deploy is highly dependent on your network topology and characteristics and pattern of usage of its users. You need to consider not only the number of users but also their location on the network and the cost of placing additional conferencing traffic on the interconnecting network. In addition, you need to consider the level of redundancy for fault tolerance and service performance requirements.

The following criteria affect the deployment architecture for data conferencing:

- Windows 2000 Site Architecture
- Placement of Conference Management Services
- Corporate network topology and bandwidth characteristics
- Network location of conferencing users
- Requirement to conference with users across a firewall
- Bridging of videoconferences

# Windows Site Architecture

Exchange Conferencing Server uses the Windows site as the outermost topology construct that defines the locality of both server and users on the network and connectivity between them.

The DCS uses the Windows site architecture to associate users with a network locality.  It will target them towards specific T.120 MCU when they want to join a conference.

The Windows site architecture is constructed using the Windows Sites and Services administration utility.  If your Windows organization is using any form of directory replication, this architecture will already be defined.  Typically, a site defines the sub-net addresses of the machines on your networks that are interconnected by high bandwidth and persistent connections. If this is not true, then additional care must be used when installing conferencing servers into these sites to ensure all conferencing servers to still meet these criteria.

With the CMS being the top-level server within an ECS installation, the Windows site in which its host machine is installed defines a root node of data conferencing servers.  The DCS code always resides on the same machine as the CMS. Together, the CMS and installed conference technology providers, such as the DCS, define the Conferencing Site.  The Conferencing Site is also the unit of management access through the ECS administration utility.

The servers that host the T.120 Multi-point control units are then defined relative to a Conferencing Site and the Windows site in which it resides.

When an MCU is first installed on a machine, it will attempt to be automatically assigned with any Conferencing Site already defined within the Windows Site.

# Placement of Conference Management Services

As described in the section about the CMS, multiple such Conferencing Sites can exist within your organization. The DCS leverages this multiple conferencing site architecture to provide a top-level decision on the preferred network locality of a user requesting to join a conference. When a user requests to join an online conference scheduled at one location, the DCS considers whether a Conferencing Site exists at their location. If the Windows Site in which the user exists contains any T.120 MCU, the users of that Windows site will be referred to that Conferencing Site.

Inter-Site Referral is configured on a per Conferencing Site basis and is effected by configuring T.120 MCUs as able to accept client or server connections from remote sites. Since this configuration allows a different network name to be used for these connections, the Conferencing Site topology can be deployed within an organization in which either the firewall or the network addresses isolate Windows Sites.

# Corporate network topology and bandwidth characteristics

The remainder of this section goes into details with respect to different characteristics of network connectivity. The cost of network bandwidth between Windows Sites and sub-nets within a site affect the deployment locations of T.120 MCU servers. These MCUs can be used to concentrate the unicast client connections in a conference to a single server and then the DCS will interconnect these MCUs in a single conference with a unicast connection across the Window Site or sub-net boundaries. This automatic single instancing of conferencing data defines much more scalable and more efficient network bandwidth consumption model as compared with other existing data conferencing solutions.

# Network location of conferencing users

There are three aspects to attaching a conference user to their closest T.120 MCU:

- Is the user attempting to join a conference from a remote location that also has Conferencing Site installation;
- Is the user attempting to join a conference from a location that is defined as local to this Conferencing Site;
- Has the administrator defined visibility restrictions on which MCU a user can connect

When a user from a conferencing site attempts to join a conference on a different conferencing site, the hosting Conferencing Site will refer the user to their local site and facilitate the interconnection of the two sites. This creates a single instance of the conferencing data between the two locations.

If a user attempts to join a conference from a Windows 2000 site that does not have a Conferencing Site deployed and if their site has been given affinity to an MCU in a different site, the user will be considered to be within that site. Otherwise, they are considered remote to the hosting site and will be attached to an MCU configured to accept remote connections on the hosting site.

Through administrative settings, it is possible to restrict access to an MCU based on a set of sub-net address masks. Only users whose IP address matches a defined sub-net are given the option of joining such MCU. This allows the administrator to sub-divide the Windows 2000 site and target users to specific MCU.

# Requirement to conference with users across a firewall

The data conferencing provider allows the T.120 MCU to be deployed in an organizational network that contains two level of security firewall:

- A firewall between the intranet and Internet
- A firewall around a Windows 2000 site

Each MCU can be configured with a different network name that is used by clients that attempt to connect to the MCU from each of the three regions separated by these firewalls.

All users within the local Conferencing Site will use the local network name, users remote to the Conferencing Site use the remote network name, and users from the Internet use the Internet network name. These name separation enables two mechanisms for bridging the security regions. The simplest is to multi-home the MCU and connect each network card to the separate network region. Then configure each network name to be the IP address, or associated DNS name, of each of these Network cards. Clients that then attempt to join conferences from each region will be given the network address of the network card for which they have access.

Alternatively, some firewall products can be configured to implement a reverse packet filter for the T.120 connections on port 1503 and target such connection requests to the MCU. In this case, the MCU would be connected solely within the Intranet and the external clients would refer to the MCU with the network name of the firewall.

# Bridging of Videoconferences

When a data and video Conferencing Resource is booked for a conference, it is possible to bridge the multicast videoconference to H.323 NetMeeting clients on down-level platforms or multicast incapable networks.

When a user attempts to join the data and video online conference, the conference access pages will first discover the client’s capability to join the multicast videoconference directly. If possible, the user will be placed into the multicast

conference and enjoy the full features of the VCS.  Clients whose machines are unable to join the conference in this manner, if administratively enabled, will connect with the T.120 MCU as normal, but in addition, request that a H.323 unicast call be bridged into the multicast videoconference.

For other multicast conference participants, this H.323 client looks and sounds like any other multicast participant.  The H.323 client will hear each participant of the conference, as would any multicast participant, however it will receive only a single video image.  The selected image is chosen based on the participant of the conference that is considered to be actively speaking.

Since only a single video stream is sent to/from the H.323 client, users with slow links, connecting to the conference via ISDN BRI channels and even 56 Kb modems will be able to participate in videoconferences.

To improve performance, you will want to install more than one MCU on the portion of your network where you have many simultaneous users. The MCUs in this area may have the same scope mask restricting client access to the specific subnets or none at all, since the site's CMS will automatically load balance among the MCUs. For more information on configuring MCU scopes and visibility, refer to the ECS online documentation

When bridging H.323 clients with VCS multicast conferences is enabled, all MCUs that are expected to accept H.323 client connections must have multicast connectivity among themselves.

# Site Architecture

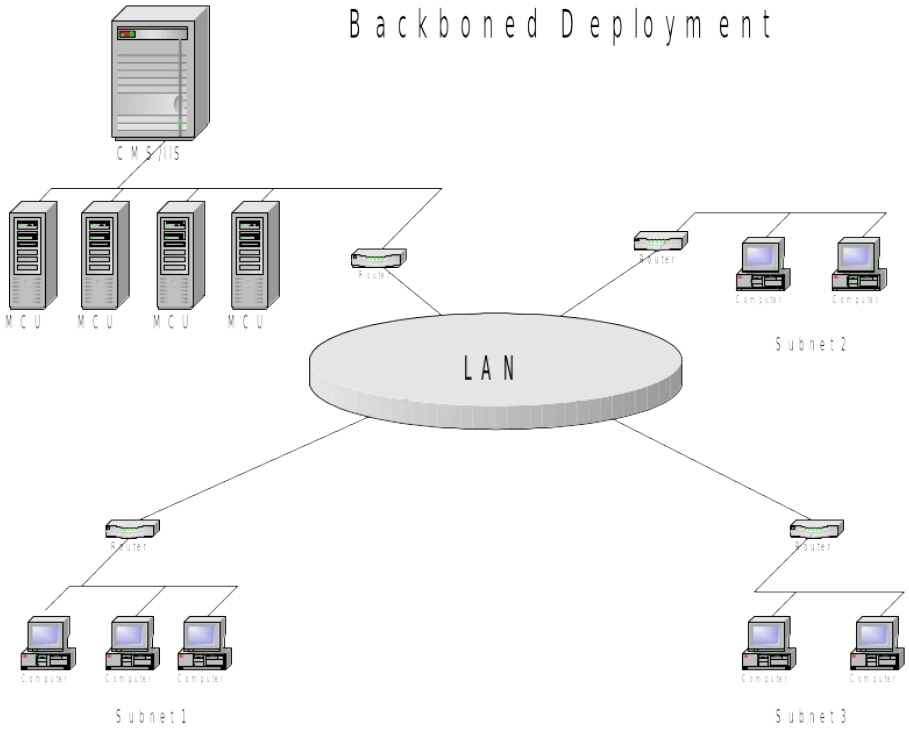
Each MCU can be configured to restrict user access to its conferences in several ways. By default, a MCU is configured to not allow connections from the Internet but doesn't have any restrictions for local and remote connections and the logic for finding the 'best' MCU described above applies. A MCU is capable to distinguish user connections from a local site, remote site and the Internet. Any MCU can be configured to restrict/allow access from any of these visibility categories. In addition, a set of network addresses can be configured for any combination of these categories that impose the MCU to reject connections from clients that don't belong to any of defined subnets. The rejected clients will be referred by the DCS to the next 'best' MCU available in the organization.

Another MCU setting that defines the logic of the users connections algorithm, is the affinity to a Windows 2000 site. This optional setting defines the MCU that is preferred to accept the user connections from a particular Windows 2000 site that doesn't have its own ECS.

Given all this complexity, but also the flexibility of the DCS topology definitions, it is important to determine your priorities and develop the deployment strategy that best suits your requirements, network infrastructure and usage patterns.

Do you care more about your network load than the fault tolerance of the service? Is flexibility more important than optimal Conference Resource allocation? These issues and possible deployments are considered in the following examples.

# Backboned Network




Consider a deployment in which all clients have a low-cost, high-bandwidth connection to a centralized network infrastructure. This kind of network would normally already deploy network services all together such as email and database service in a network-central, data-center. In this case, the components of the Conference Server would also all be placed in that location. Multiple T.120 MCUs would be installed to load-balance and provide redundancy for all network clients.

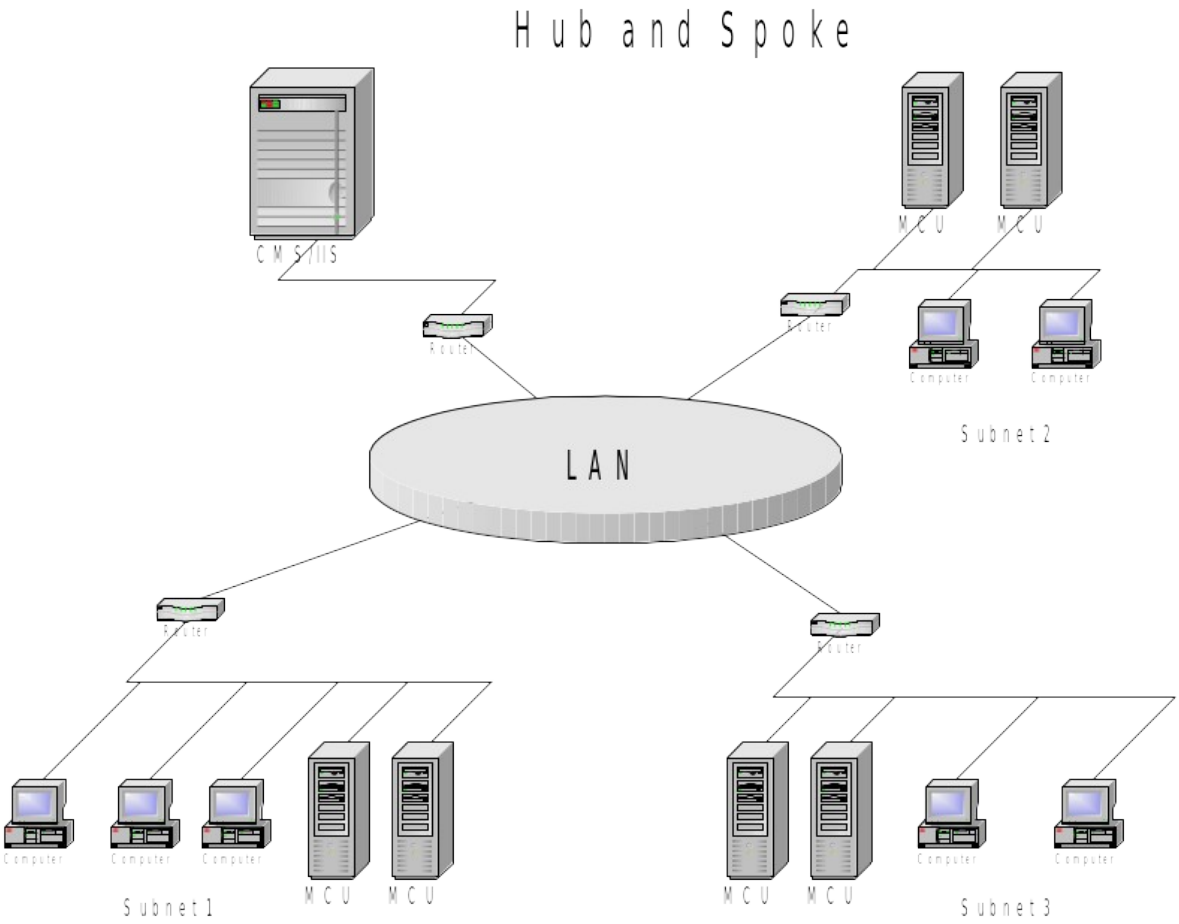
Implement Backbone deployment if you are planning to deploy DCS on only one Windows 2000 site and the inter-subnet traffic is not a major concern. As you can see from the diagram, the backboned topology places the CMS and all the MCUs on the corporate backbone network. This allows for better resource management, load balancing and fault tolerance but increases network traffic between subnets. As an additional gain, with this topology, administrators get better control and manageability.

**Note** For simplicity, on this and following pictures, IIS is shown to be on the same server with CMS. This doesn't have to be the case: the only requirement is to have IIS running on the same site with CMS.

# Hub and Spoke

If inter-subnet traffic is an issue, consider hub and spoke topology, setting the CMS in the hub and placing one or several MCUs on the subnets where conferencing users are expected to be.

This layout ensures that conference traffic traverses subnets over a single link. However, better network load may be compromised by poor load balancing and fault tolerance. A hub and spoke topology can be much more efficient than the backboned one, when most of conference participants are from the same subnet. In this case, most of the data conferencing traffic happens within the subnet.

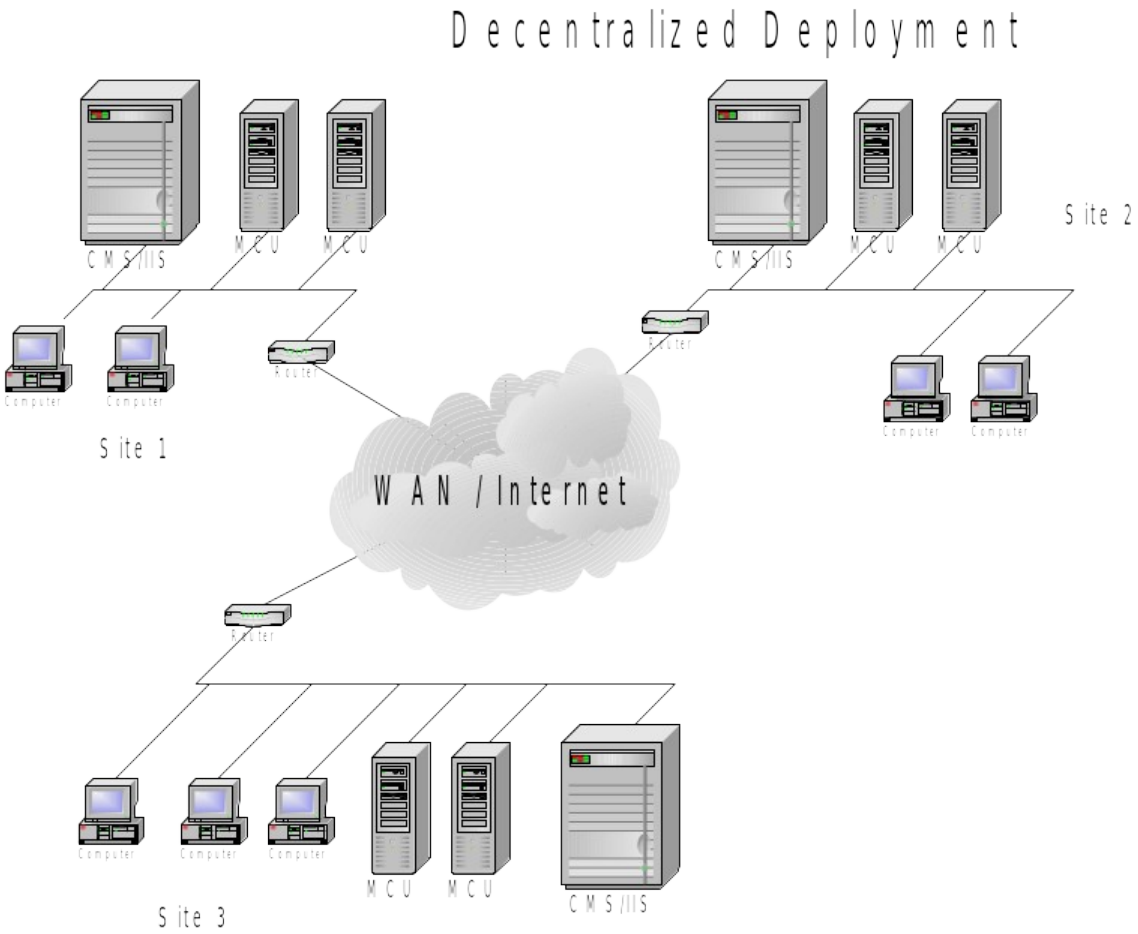



# Deployment in Multiple Sites

If you have multiple sites, each with multiple users potentially attending conferences at the same time, you should consider decentralized deployment. As shown on picture[1] below, in each site, there is a CMS and one or more MCUs. If there are firewalls between the sites, a proxy MCU must be defined on each site.

If you want to limit the inter-site bandwidth usage even further, you can dedicate a single MCU on each site for remote connections. This will ensure that, no matter how many conferences are happening across the sites, only single conferencing traffic occurs between any pair of sites. For more information on how to configure MCU scope and visibility refer to the ECS online documentation.

When planning a decentralized deployment, take into account that conferencing resources on each site are reserved only by conferences scheduled inviting Conference resources in that site. If users participate in data conferences




scheduled/happening on remote sites, they are connected to local MCUs but their usage of MCU capacity is not reflected in resource availability on that site. Thus, if you expect large number of inter-site conferences, use conservative approach for setting the limit of total number of simultaneous connections when configuring the DCSs on those sites. For more information about configuring DCS, refer to ECS online documentation.

[1] For simplicity, firewalls and other elements of network infrastructure are omitted.

# MCU Connections and Types

As was described in previous sections, there is a great flexibility and large number of possible combinations of MCU visibility settings possible. To simplify this complexity, it is convenient to classify MCU types by their purpose. Here is the list of most common types of MCUs you can deploy in your organization depending on the specifics of your network and usage:

**Local MCU** is an MCU that accepts only connections from user machines in the same Windows 2000 site. To configure a local MCU, you will need to disable 'accept remote connections' (remote visibility) and 'accept Internet connections' (Internet visibility) and enable 'accept connections from the local site' (local visibility) settings on the MCU property sheet.

**Local MCU with subnet scope restrictions** is a local MCU that accepts user connections only from explicitly defined subnets in the site. It is configured by checking the appropriate 'Restrict visibility' checkbox on the MCU property sheet and adding network address/subnet mask pairs on the visibility tab. For more details on configuring MCU visibility settings refer to the ECS online documentation.

**MCU with site affinities** is an MCU that treats connections from specific Windows 2000 sites as local. This setting allows the administrators to denominate an MCU that presumably has faster connection to a particular site as the preferred for the users of that site. You configure this by pressing the 'Sites' button on the MCU property sheet and adding affinities from the list of available sites.

**Inter-site connector MCU** is an MCU that serves as a bridgehead between remote Windows 2000 sites. Such an MCU will accept connections from remote MCUs and individual remote users if ECS is not available on their sites. If you want to dedicate an MCU to the inter-site connections only, disable the local and Internet visibility on the MCU property sheet.

**Internet connector MCU** is an MCU that accepts connections from the Internet users. Analogously, you configure this by enabling Internet visibility and, optionally, disabling local and remote visibility settings.

**Inter-enterprise MCU** is an MCU configured to accept connections from the specific networks on the Internet. This is useful when you decide to have conferences with specific organizations over the Internet. To set this type of MCU, you need to enable Internet visibility, check 'Restrict visibility' for the Internet connections and add appropriate Network address/Subnet mask pairs on the MCU visibility tab.

For your specific requirements, any of these settings can be used in combination with others. For more details on configuring MCU, refer to the ECS online documentation.

**Important note:** If you configure an MCU to be visible from the Internet, and you have only one Windows 2000 site defined in your organization, you must create the second Windows 2000 site and deploy the Internet visible MCU it that site, otherwise Internet users will be treated as local by the DCS.

# Security Model

## Firewall traversal

DCS can be configured to support conferences with Internet or remote site participants connecting over the corporate or site firewall. The standard approach to this would be configuring an MCU on the firewall with Internet/remote site visibility and two network cards/IP addresses installed. Make one of the IP addresses visible to the Internet/remote sites and the other accessible to the local site. The TCP port 1503 must be enabled for the outside traffic for T.120 packets to get in. Using the MCU property sheet settings, you may also define different network names for the MCU, for the local and remote users. You may impose additional restrictions on the network addresses from which the MCU will accept connections.

If your firewall allows for packet filtering and forwarding, you may deploy the MCU with external visibility inside the firewall and configure your firewall to forward T.120 traffic.

## Support for secure online-conferences

**Important** Users who want to participate in secure conferences must use NetMeeting 3.01 or higher and use Microsoft Internet Explorer. For more information, see “Client Software” later in this chapter.

To support secure conferences, you must install Microsoft Certificate Services on at least one server in the domain. Certificate Services provides a certification authority (CA) that renders certificates to users allowing their authentication for secure conferences.

## Client Certificates

A digital certificate is an electronic document that grants credentials to the users or computers on the network.

It is issued by a certification authority (CA). It contains name, a serial number, expiration dates, a copy of the certificate holder's public key, email address and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. The most widespread standard for certificates is X.509.

The certificates are necessary for users who want to join private data conferences. The DCS recognizes certificates that are granted from ‘trusted CA’ in the organization. A Windows 2000 certificate server must exist in the active directory forest of domains. MCU queries the certificate server to obtain a machine certificate that it uses for authentication with the clients. MCU uses Windows Crypto API that scans active directory and local registry for the list of certificate authorities that are considered valid in the organization. MCU then compares client certificates against this list to validate user’s authenticity.

If you want users with the certificates granted by third parties, such as VeriSign, partake in secure conferences, you would need to make sure your organization is subscribed to the third party certification services and the hierarchy of trusted CAs are properly configured. For more information on configuring certificate services, see Windows 2000 online documentation.

# Reliability Planning

To increase the reliability of the data conferencing services in your organization consider deploying more than one MCU accepting connections from the same groups of users. There is no need to place MCUs in a cluster: the DCS will provide automatic fail over for the MCUs in the site.

When placing MCUs in your network, ensure that each of them has fast connection with the active CMS server in the site, since MCUs periodically and during the conference exchange DCOM calls with the DCS.

ECS audit and application logs and performance monitor counters can serve as a valuable source of information for assessing current reliability of your DCS infrastructure. In particular, the MCU application logs will give you a statistics on the number of software, hardware and network failures, MCU service downtimes and more. The performance monitor counters will give you an idea on what are the connection speeds and how big is the DCOM traffic. For more information on performance counters, see ECS online documentation.

# Scalability and Performance

The audit log files and performance monitor counters can give you valuable information on the MCU load dynamics, average connection delays and various other performance characteristics of your DCS configuration. This information can be used to plan how many and what type of MCU servers to deploy for optimal performance/resource utilization.

The DCS logic is highly scalable and allows you to increase number of MCUs in the site. However, you will have to make a tradeoff between the number of MCUs and individual server performance. If you deploy many MCUs accepting connections from the same groups of users using relatively low performance servers, DCS will automatically balance the load choosing the MCU with the lowest load as a hosting MCU for the conference. Thereafter, it will connect all the local attendees of that conference to the same MCU to minimize number of hops for the conference traffic. This will continue until a configurable threshold for the MCU load is reached, after which the new connection requests will be redirected to another available MCU that has the lowest current load.

Thus, deploying an MCU on a bigger machine will produce conferences that, on the average span over the smaller number of MCUs, therefore causing smaller delays for the conference payload traffic. If you deploy higher number of smaller MCUs in the site, you will get higher reliability and fault tolerance.

# Deploying Data Conferencing

## Server Minimum Requirements

Minimum system requirements for an MCU server are those of Windows 2000 Server. As a guideline: a server with Pentium 400 MHz, 256 Mb RAM, can handle at least 500 simultaneous user connections.

## Clients

In order to participate in a DCS conference, client computers are required to have two components installed: any client software that supports T.120 standard and

any Internet browser that supports JavaScript and frames. For the best experience, it is recommended to use NetMeeting 3.01 and Internet Explorer 4.01 or higher. In particular, these are the minimum requirements for participating in secure DCS conferences. Also, this configuration will embed NetMeeting into the web page, given your browser security settings do not prevent running ActiveX controls.

If you use lower versions of NetMeeting, (but not lower than 2.0), NetMeeting will be automatically launched as a separate application and connection with the conference automatically established.

If any of those versions of NetMeeting is not found on the client machine, a dialogue box asking the user to start T.120 client application will be displayed. Users are required to manually start the client application and hit OK on the dialogue box. This will cause the MCU to attempt initiating T.120 connection with the client.

Netscape users will have the same experience as described in the previous paragraph.

**Note:** Since the MCU/client connections use IP addresses it is important to configure your proxy settings to bypass proxy server5s for local addresses.

# Exchange Video Conferencing Service

## What is Video Conferencing?

Videoconferencing is a technology that allows two or more people at remote locations to exchange their voices and video images in real time. NetMeeting has some limited videoconferencing capabilities. For example with NetMeeting 3.01, you can establish a peer-to-peer videoconference using ITU-T H.323 unicast standard.

The Exchange Videoconferencing Service allows users to organize and participate in multiparty video and audio conferences. VCS technology is a based on the IETF IP multicast standards. In addition, VCS conferences are available for clients with H.323 capabilities, such as NetMeeting, over an IP multicast/H.323 unicast bridge that is part of the ECS and can be deployed on a separate MCU server. Thus, the VCS combines greater efficiency on multicast enabled networks with wider accessibility and low bandwidth support over non-multicast networks, such as Internet.

### Joining a conference

When users hit ECS conference access URL, an ECS default active server page (ASP) on the IIS requests the CMS to locate the conference profile and return the URLs of CTPs associated with the conferencing resource booked for that particular conference. The user's Internet browser window then is divided into number of frames: one for the generic conference information and controls, and one for each CTP. What happens then in the CTP frame and behind the scenes, on the network, is entirely up to that CTP.

In case of VCS CTP, a script starts on the client computer that investigates whether client configuration and network connectivity characteristics would allow joining directly to a multicast conference. If any of the prerequisites are missing, an attempt will be made to connect the user to the MCU over a unicast H.323 connection. This fallback call be disabled on the per-resource basis.

If a multicast connection is established, users will be able to see multiple participants' video and hear up to five active speakers simultaneously.

In case of H.323 connection, the user will still hear up to five active speakers, but see only one - the current speaker. However, they will appear as any other participant's video on the multicast clients' screens.

**Note:** The H.323 bridging is available for only the combined conferences with both VCS and DCS technologies present. The actual H.323/multicast bridging is accomplished over the DCS MCU servers. The bridge is installed as a part of T.120 MCU component installation.

### How VCS works

When a conference with a VCS resource starts, a special multicast IP address is requested from a MADCAP server and reserved for the conference. This address cannot be used in the following reservations until the initial reservation expires. The expiration time is defined as the maximum videoconference extension time

plus the scheduled conference end time. The maximum videoconference extension time is configured from the VCS property sheet and defines the maximum time, in minutes, for which an already started conference can be extended by the conference organizer.

When a user joins a VCS conference as a multicast client, his or her multicast client ActiveX control receives the multicast IP address reserved for the conference from the VCS. The control then ‘subscribes’ to the multicast conference and starts retrieve/send video and audio payload from/to that multicast address.

In the pure multicast videoconference, there are no servers that participate in actual video/audio traffic transfer. If there are routers in the way of the multicast packets, they serve as replicators/multiplexers forwarding packets to the network segments where clients ‘subscribed’ to the conference are located.

In the network, MADCAP servers must exist and the routers must be multicast aware for a multicast videoconference to work.

# What is MADCAP?

MADCAP (previously known as MDHCP) allows a unique multicast group IP address to be obtained for each Exchange videoconference. MADCAP is part of the Windows 2000 DHCP service. Windows 2000 DHCP servers can optionally also handle assignment of multicast addresses, in addition to unicast addresses. You configure multicast scopes and the corresponding multicast IP ranges on the server through the DHCP console. This is required before an Exchange Video Conference can be successfully scheduled and conducted. Once these scopes are administratively set and activated, the Windows 2000 DHCP Service can provide multicast addresses in the same way it normally provides unicast IP addresses where DHCP scopes are used.

> **Note** Although MADCAP is packaged with the DHCP service; DHCP and MADCAP are independent of each other. You can use a MADCAP server to provide multicast addresses, and run DHCP on other servers on your network.

**Configure MADCAP for Exchange Video Conferencing**

- Install the DHCP service, if it is not already installed.
- Use the Windows Component Manager to install MADCAP. The component name to be installed is **Dynamic Host Configuration Protocol (DHCP)**, from the **Network Services** group. (The MADCAP service is implemented as part of DHCP).
- For networks using domains, you must authorize the DHCP service in the domain’s directory service database. This prevents users from setting up unauthorized DHCP services. This is not necessary if the server has been authorized already (for example, if it is already functioning as a DHCP server).

- To have the DHCP server allocate multicast addresses using the MADCAP protocol, create a new multicast scope. For more information on creating a multicast scope, see “Manage Multicast Scopes” in Windows 2000 online help (location: DHCP).
- After creating a new multicast scope, associate each scope with a TTL (time-to-live) value of your choice. For more information on setting the TTL value on

a multicast scope, see “Manage multicast scopes” in Windows 2000 online help (location: DHCP).

# What is IP multicast?

IP multicast is an extension to the IP network-layer protocol defined in RFC 1112, in 1989. It provides an efficient way of transmitting packets in the network from one or more sources to many destinations.

There are three basic modes of transmitting packets over an IP network: unicast, broadcast and multicast. Unicast transmits packets over a point-to-point connection. If there is more than one recipient for the packet, several point-to-point connections has to be established and a copy of each packet is sent to each recipient.

In broadcast mode, a single copy of a packet is sent to the entire network, including subnets that don’t have recipients of the packet. Thus, extra traffic is created consuming valuable network bandwidth.

The third mode of transmitting, multicast, combines advantages of both, unicast and broadcast technologies transmitting a single copy of a packet/datagram to only those subnets that have recipient hosts “subscribed” to the session. Hosts subscribe to the session by joining a multicast group, which is accomplished by propagating (via IGMP protocol) a pair of addresses, multicast address and recipient’s IP address, to the routers on the network.

# What is a multicast address?

Class D IP addresses, in the range 224.0.0.0 to 239.255.255.255 are called multicast addresses.  Packets sent to an address in this range are not addressed to a specific host. Any host that has knowledge of a specific multicast address can “join a multicast group” identified by this address. This action tells the routers (via IGMP) to forward all packets that it sees to the subnet on which the host lives. The host can then pick up the packets destined to that address. A host can become a member of any number of multicast groups.

# What is TTL?

It is not a good idea to distribute all packets sent to all multicast addresses throughout the world. Multicast packets have a specific lifetime. The TTL (Time-to-live) value identifies the lifetime of these packets. Every time a router is hit in the path of the packets, the TTL value is reduced by one, and if the value is zero, the router does not forward the packets any further. This immediately means that packets with TTL value of 1 are distributed within the subnet only. Multicast datagrams with a TTL of greater than one may be delivered to more than one subnet if there is one or more multicast routers attached to the first-hop subnet.

# What is a multicast group?

An IP multicast group, also known as a host group, is a set of hosts that listen for IP traffic destined for a specific multicast IP address. Multicast IP traffic is sent to a single MAC address but processed by multiple IP hosts. A given host listens on a specific IP multicast address and receives all packets to that IP address.

The Internet Group Management Protocol (IGMP) is responsible for the management of IP multicast groups.

The membership of a host group is dynamic; that is, hosts may join and leave groups at any time. There is no restriction on the location or number of members in a host group. A host may be a member of more than one group at a time.

A host group may be permanent or transient. A permanent group has a well-known, administratively assigned IP address. It is the address, not the membership of the group that is permanent; at any time, a permanent group may have any number of members, even zero. Those IP multicast addresses that are not reserved for permanent groups are available for dynamic assignment to transient groups that exist only as long as they have members. Members of a host group can span IP routers across multiple networks. This situation requires IP multicast support on the IP routers and the ability for hosts to register their group membership with local routers. Host registration is accomplished using IGMP.

For a host to receive IP multicasts, an application must inform the local router that it will be receiving multicasts at a specified destination IP multicast address. If the network technology supports hardware-based multicasting, then the network interface is told to pass up packets for a specific multicast address. In case of Ethernet, the network interface card is programmed to respond to a multicast MAC address corresponding to the desired IP multicast address.

In order to facilitate IP multicast between subnets, the routers must be multicast aware. Routers maintain special routing tables enabling them to make a decision whether to forward multicast traffic to the specific network or not. Routers propagate routing information and create a router topology known as spanning tree, for each multicast session. The spanning tree is constructed in a way that only single path exists between any pair of participating routers and there are no loops.

# What is a multicast scope

- A range of multicast addresses and an associated TTL define a multicast scope.  The scopes used for videoconferences are retrieved from the scopes defined on the organizations MADCAP servers. Using scopes, in conjunction with configuration of routers it is possible to limit the reach of multicast packets on the network.

# Reserved addresses:

The following table is a partial list of Class D addresses reserved for IP multicasting and registered with the Internet Assigned Numbers Authority (IANA). These are the addresses of the permanent well-known groups that are mentioned in the previous section.

| Multicast group | IPmulticast address | Description |
|---|---|---|
| Base address | 224.0.0.0 | Reserved |
| All hosts | 224.0.0.1 | Contains all systems on the same physical network |
| All routers | 224.0.0.2 | Contains all routers on the same physical network |

| | | |
|---|---|---|
| Network Time Protocol | 224.0.1.1 | Distributes time-clock data used to synchronize time on a group of computers |
| RIP version 2 | 224.0.0.9 | Distributes routing data between a group of routers that use a version 2 raster image processor (RIP) |
| WINS server | 224.0.1.24 | Supports auto-discovery and dynamic configuring of replication for WINS servers |

A multicast router does not forward multicast datagrams with destination addresses from 224.0.0.0 through 224.0.0.255, inclusive, regardless of their TTL value. This address range is reserved for routing protocols and other low-level, topology discovery protocols, or maintenance protocols. These include gateway discovery protocols and group membership reporting protocols

# How to use Scope/TTL to limit video on your network

When deciding the IP address ranges to use for multicast scopes on your MADCAP server, there are two overall best practices recommended by the Multicast Allocation (malloc) working group, an IETF team of industry volunteers who help set multicast address allocation standards. These practices include:

- **Administrative scoping** is most useful when you are using multicast IP addresses privately within your own network. With administratively scoped multicast IP, it is recommended that you start using the **239.192.0.0** range. This range is known as the IPv4 Organization Local Scope and uses a subnet mask of 255.252.0.0 (14-bits in length).

  **Note** Administrative scoping is fully discussed in RFC 2365, “Administratively Scoped IP Multicast.”

- **Global scoping** is most useful when you are using multicast group IP addresses in a public network address space, such as the Internet. Global scoping is not available in Exchange 2000 Video Conferencing.

# Reliability Planning

## Checking routers on your network

Use the MCAST diagnostic tool included with the Windows 2000 Resource Kit to determine which parts of your network are enabled for transmission of IP multicast packets. Use the tool in ‘send’ mode to set up multicast sources at different locations on your network. Use it in receive mode to determine where multicast traffic is being received. For more information, see “Enabling IP Multicast” in Windows 2000 online help (location: Telephony). Windows 2000 also provides utilities to display the configuration of a multicast router (mrinfo), and to display multicast group tables and troubleshooting information for interfaces (routemon). For more information, see “Using the IP multicasting utilities” in Windows 2000 online help (location: Routing and Remote Access).

## Configuring multiple MADCAP servers

Configuring multiple MADCAP servers may be a good idea for the reliability and network efficiency reasons. If you more than one MADCAP in your network, you must make sure the multicast IP scopes configured on the servers do not overlap. Also, since each of the IP scopes is also associated with lease expiration period and advertising scope settings, it is a good idea to configure each type of multicast IP scopes you are planning to have on two or more MADCAP servers. This will allow you to put down a MADCAP server without compromising the ability to lease multicast addresses of any particular kind.

Lease expiration period and advertising scope settings are discussed in further details in the “Resource Property Settings” section, later in this chapter.

# Configuring routers on your network

If there is a router on your network and you want to enable multicast conferencing across the router, you may have to configure your router to handle multicast packets. For example, you must create access lists specifying the range of multicast group addresses allowed to cross the router, and associate these lists with specific interfaces on different routers. For more information, see “Enabling IP Multicast” in Windows 2000 online help (location: Telephony).

Detailed information on configuring your router may be available from your router vendor, or from their web site. Certain publications also contain information describing configuration of routers and how the underlying protocols work.

**Note:** For example, enabling multicast on Cisco routers is covered in “Cisco IOS Solutions for Network Protocols, Volume I: IP”, Cisco Press, 1998. ISBN 1-57870-049-3, Chapters 24-25.

# Resource Properties Settings

After you create a conferencing resource you need to associate one or more CTPs with the resource. Each CTP will, generally, have some properties associated with the resource that will define specific characteristics of the conference scheduled against that resource.

The following properties can be defined for the resources associated with the VCS CTP:

**Resource size** is configured by defining “Limit number of participants to:” setting on the resource’s VCS property sheet. This setting accepts an integer that sets a maximum number of attendees that would be able to send audio/video to the conference.

Note the difference between the interpretation of the ‘size’ property by DCS and VCS: if a data conference already has allowed number of attendees in the conference, new connection attempts will be rejected and users will not be able to get into the conference. If this happens with the VCS conference, the extra attendees will be allowed to the videoconference as observers, but will not be seen or heard by other participants.

**Audio CODEC payload type** defines the standard for audio stream encoding. Each CODEC type has, generally, different impact on the used network bandwidth and client CPU load. As a rule, a CODEC that uses less bandwidth requires more

CPU time on the client machine to encode and decode the audio payload. For more information on supported CODEC types and their properties, refer to the Windows 2000 online documentation.

**Automatically send client audio at join time**, when unchecked, will prevent users' audio streams to be sent to then conference when they join. Users then have option to turn on audio during the conference if they need to be heard. This setting is useful for the conference resources with a big size that are used for conferencing scenarios where one or few people talk most of the time, and there is a large number of observers who must be able to "chime in" time to time with questions or comments. Disabling their audio transmission at the time they join, mitigates possible surges in the network and reduces possible interruptions in the main presenter's audio stream.

**Enable video** setting, when turned off, defines audio-only conferencing resource. Audio-only conferences consume significantly less network bandwidth and are appropriate for many routine scenarios where images are not crucially important.

**Video CODEC payload type** property is similar to the Audio CODEC property and similar considerations, but applied to video, are valid.

**Image size** can be set to either default Quarter Common Intermediate Format (QCIF) or Common Intermediate Format (CIF). This property defines the size, in pixels, of the video frames transferred/displayed in a VCS conference. QCIF defines a video image of 176x144 pixels and CIF 352x288 pixels. When changing this setting to larger size make sure that users' cameras are CIF capable, otherwise their video images may appear four times smaller. Also, when configuring a CIF resource, remember that CIF format consumes significantly more network bandwidth and CPU power than QCIF.

**Automatically send client video at join time** is similar to the analogous setting for audio and is aimed at similar scenarios and network surge protection.

**Multicast IP scope** property can be configured by selecting one ore more entries from the "Use multicast IP addresses from the following scopes" list box on the conference resource's VCS property sheet. Each entry in the list box represents a named scope configuration that VCS reads from the existing MADCAP servers. Each scope configuration is associated with a specific IP scope as well as two other multicast properties set on a MADCAP server, specifically:

**Multicast IP address expiration period** – is the maximum period of time for which a multicast IP address can be leased out. If the multicast IP address is requested from that scope, it will be leased for a period not exceeding the maximum setting for this scope on the MADCAP server.

**Advertising scope** – is the time-to-live (TTL) value for the multicast packets, or the maximum number of hops that the packets will travel over the network, before being dismissed by routers. This setting may be used to limit VCS conferences to specific network segments.

By default, no specific scope is selected and VCS will generate multicast IP addresses randomly. Randomly generated addresses are not guarantied to be unique, thus, there can be situations when two or more videoconferences will be visible to one another. For this reason, it is recommended to always have an active MADCAP server available and multicast IP scope property configured on all VCS resources. This will ensure that VCS will request multicast IP addresses from MADCAP servers and each such address will be unique.

If several multicast IP scopes are selected from the list box, the VCS will use the first successfully fulfilled request. If all the multicast IP address requests fail, the address will be allocated randomly.

# Network considerations

To use Exchange Video Conferencing, your network needs to be multicast-enabled and you need to specially configure multicast addresses. If this is the first IP Multicast deployment in your enterprise, reconfiguration of some of your routers may be required. However, if you have previously deployed multicast applications such as NetShow, your network may already be multicast-ready.

IF your network routers support Resource Reservation Protocol (RSVP), the quality of service (QoS) policy may be configured for each subnet or for whole network to allocate and guarantee network bandwidth for the VCS multicast traffic. The policy is configured using Windows 2000 QoS Admission Control management console (MMC). For more details on how to configure QoS policy, refer to Windows 2000 online documentation.

When making decision on the maximum size the simultaneous connections and when determining QoS policy, take into account the bandwidth of your network and the manner in which the VCS will be used in your organization. Are there going to be meetings that require all the participants send both, video and audio during the conference? What will be the expected portion of audio only meetings, presentations? Try to calculate the expected and peak video/audio traffic on the network. Dependent on CODECs used, every audio stream will consume from about 21 Kbps (GMS 6.10 CODEC) to about 74.7 Kbps (G711). These numbers include the IP header overhead.

The video streams, aside from the CODEC, are highly dependent on the amount of movement in front of a camera. As a rule of thumb, expect about 60 to 120 Kbps consumed by a video stream, and this number increases less than linear with the number of attendees in a conference

.

The H.323 clients are sending and receiving a single video and a single audio streams in/from a VCS conference.

Both multicast and H.323 clients can use Remote Access Services (RAS) to join VCS conferences over a dial up connection using 56 Kbps modems or ISDN. For multicast connectivity the RAS server must run Windows 2000 Server OS and IGMP service needs to be active.

# Deploying Video Conferencing

## Minimum Requirements

The minimum multicast client hardware requirements are those of Windows 2000 Professional. Sound card with microphone and speakers and a video capture card or camera are also required.

The minimum requirements for H.323 clients are:

- NetMeeting 2.1 and above

- For Windows 95, a Pentium 90 processor with 16 MB of RAM (a Pentium 133 processor or better with at least 16 MB of RAM is recommended).
- For Windows NT, a Pentium 90 processor with 24 MB of RAM (a Pentium 133 processor or better with at least 32 MB of RAM is recommended).
- 4 MB of free hard disk space
- 56,000 bps or faster modem, ISDN, or LAN connection.
- Sound card with microphone and speakers
- Video capture card or camera.

# Clients

Multicast clients require a Windows 2000 OS. The clients are ActiveX controls running in the VCS frame of the Internet browser. Make sure your browser security settings allow a control to be downloaded and run on the client machines. If you organization policy doesn’t allow download of ActiveX controls, you may copy and register controls manually as described in the “Optional manual install of client components section” earlier, in this book.

H.323 clients will require H.323 client software, such as NetMeeting 2.1 or higher.